Report: 27 August 2025

Australian Bureau of Statistics

CENSUS 2026 PRIVACY IMPACT ASSESSMENT (PHASE 3)

IIS Partners
INFORMATION INTEGRITY SOLUTIONS

IIS Partners

Contents

1. Executive summary

The Australian Bureau of Statistics (ABS) engaged IIS Partners (IIS) to conduct a privacy impact assessment (PIA) of the Census to be held in 2026. This PIA forms the third and final phase of a three phase PIA process. It focuses on activities and practices that will be different in 2026 compared to previous Census cycles, with attention given to issues not covered in the Phase 1 and 2 PIAs. The PIA assesses those new activities and practices (including new approaches to personal information handling) against the requirements of the *Privacy Act 1988* (Cth). It also makes suggestions for privacy best practice and data ethics consideration.

IIS would like to thank the many people at the ABS who assisted us during the development of this PIA, along with those stakeholders who provided invaluable feedback on Census privacy arrangements.

1.1 IIS's overall view

Overall, IIS finds that the ABS is taking appropriate steps to meet its obligations under the Privacy Act in relation to the Census. Our assessment demonstrated that the ABS's internal systems and practices in relation to privacy are operating effectively – ensuring privacy is a central consideration for new projects and providing for robust privacy oversight and assurance. In particular, the ABS's system of Census Data Protection and Retention Plans has further strengthened data governance at the team level. Additionally, the ABS's program of Privacy Threshold Assessments (PTAs) and internally conducted PIAs embeds a rigorous approach to assessing privacy protections and risks in new projects or changes to data processing. IIS reviewed a number of PTAs during this PIA and found the assessments detailed and thorough.

During the analysis conducted for this PIA, IIS reviewed a range of matters including:

- Sharing 2026 Census data under the Data Availability and Transparency Act 2022 (DAT Act or DATA Scheme)
- Use of administrative data to enhance the Census dataset
- Access to a separate Census form
- Third party vendor management and privacy risks
- Post Enumeration Survey (PES)
- Census refusals process
- Recent Privacy Act reforms
- Evaluation of recommendations from 2026 Census PIA Phases 1 and 2.

1.2 Summary of recommendations

In this PIA, IIS makes six recommendations. A high-level summary of recommendations appears below, with the full recommendations appearing in the body of the report.

Recommendation 1 ***Best practice***	Ensure consistent ethics arrangements for any DATA Scheme project involving Census data sharing.
Recommendation 2 ***Compliance***	Ensure careful management of AI-related risks associated with any Census data sharing
Recommendation 3 ***Compliance***	Work with administrative data custodians so that initial collection notices make clear the disclosure of data to the ABS
Recommendation 4 ***Best practice***	Publicly address questions about administrative data use and disclosure (including clarity around restrictions on disclosure to the National Archives of Australia and restrictions on use for enforcement)
Recommendation 5 ***Best practice***	Ensure communications materials and scripts address key questions about use of a separate Census form
Recommendation 6 ***Best practice***	Ensure strong assurance of vendor privacy and security compliance

2. Introduction

2.1 Background

The ABS conducts the Australian Census of Population and Housing (the Census) every five years. The Census is the most comprehensive snapshot of the country and seeks to count every person and dwelling in Australia on Census night. It is a key source of information about small geographic areas and small population groups across the country. The Census form asks questions about every person in the country, including their age, country of birth, religion, ancestry, language used at home, work and education. The next Census will occur in 2026.

Census data can be used in a variety of ways by a diverse range of researchers. The 2021 Census data was published in a three-phased approach accessible through various Census data tools.[1] Census data is also integrated with other datasets to form the Person Level Integrated Data Asset (PLIDA) (previously the Multi-Agency Data Integration Project (MADIP)). PLIDA can provide whole-of-life insights about population groups in Australia, such as the interactions between their characteristics, use of services like healthcare and education, and outcomes like improved health and employment. Census data is not currently linked longitudinally through PLIDA.The 2026 Census will take place in an environment where privacy is increasingly important to the public and where government agencies risk backlash if the information they hold is misused, breached, or used in ways that are outside individual expectations. In acknowledgment of this, the ABS has prepared a 2026 Census PIA Plan, which commits to managing, minimising, or eliminating potential privacy impacts of the 2026 Census through a Privacy by Design approach and the commissioning of comprehensive and independent PIAs. The ABS has undertaken a phased approach to the PIAs for the 2026 Census:

- **Phase 1 PIA** – Preparation, planning and development (September 2023)
- **Phase 2 PIA** – Build and design (November 2024)
- **Phase 3 PIA** – Testing operational readiness (this PIA).

IIS undertook Phases 1 and 2 of the 2026 Census PIA and was engaged again by the ABS to undertake Phase 3 of the 2026 Census PIA, which is the subject of this report.

2.2 Scope of this assessment

For the third and final phase of the PIA, the Census Privacy Team developed a list of indicative focus areas for the PIA which IIS reviewed and reflected in project planning. Project scope focused on potential privacy risks which were not covered in previous PIAs as well as areas where there have been changes or developments since previous PIAs. The topics within scope for this assessment include:

- Sharing 2026 Census data under the DAT Act
- Use of administrative data to enhance the Census dataset

[1] See ABS, Census 2021 product release guide.

- Access to a separate Census form
- Third party vendor management and privacy risks
- PES
- Census refusals process
- Recent Privacy Act reforms
- Evaluation of recommendations from 2026 Census PIA Phases 1 and 2.

The following matters were out of scope for this PIA:

- Reconsideration of matters already addressed in previous PIA phases – other than evaluation of the implementation of recommendations from previous PIAs.

IIS's evaluation of recommendations from the Phase 1 and 2 Census PIAs was a point-in-time assessment in which IIS reviewed actions taken by the ABS in implementing recommendations. Generally, IIS found that the ABS had made significant headway on its implementation of recommendations with most either complete or in progress and on track. We also understand that further progress has been made on those recommendations since our evaluation. IIS provided its evaluation of recommendations as a separate attachment; the ABS advised it would take into account the evaluation as it moves to finalise PIA recommendations.

2.3 Relevant legislation

Privacy Act

The ABS is covered by the *Privacy Act 1988* (Cth) and its 13 Australian Privacy Principles (APPs). The APPs set rules for the handling of personal information which the Act defines as any 'information or any opinion about an identified individual or an individual who is reasonably identifiable' (s 6(1)). The APPs impose a range of privacy obligations on APP entities. The APPs also give individuals certain rights and choices in relation to their personal information which individuals can pursue under the Privacy Act's complaint-handling and enforcement provisions.

As an agency, the ABS is also covered by the Australian Government Agencies Privacy Code which sets out specific requirements and key practical steps that agencies must take as part of complying with APP 1.2. It requires agencies to move towards a best practice approach to privacy governance to help build a consistent, high standard of personal information management.

The ABS's legislation

The ABS is authorised to collect, compile, analyse, and publish statistics under the *Australian Bureau of Statistics Act 1975* (Cth) (ABS Act) and the *Census and Statistics Act 1905* (Cth) (Census and Statistics Act). The ABS Act establishes the ABS as an independent statutory authority, defines the functions of the ABS, establishes the office of Australian Statistician and describes the terms under which the Australian Statistician can be appointed to, and removed from, office. The Census and Statistics Act gives the Australian Statistician the authority to conduct the Census. While the ABS publishes statistical outputs, these must not be published or disseminated in a manner that is likely to enable the identification of a particular person or organisation (s 12(2)).

Practically speaking, this means that the ABS only publishes or disseminates confidentialised and aggregate statistical products. The ABS also supports controlled researcher access to de-identified unit-level Census data in its own secure environment – DataLab – subject to the Five Safes Framework.[2]

2.4 Census privacy governance

Census privacy governance remains unchanged from the Phase 2 Census 2026 PIA.

APP 1.2 promotes a Privacy by Design approach by requiring entities to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and any binding registered APP code. Relevantly for the ABS, it must comply with the Australian Government Agencies Privacy Code, which requires agencies to take a series of steps to embed privacy into their practices.[3]

The ABS has robust internal privacy governance arrangements, including a regularly monitored Privacy Management Plan, dedicated roles and committees with privacy responsibilities, privacy assessment processes, and a range of internal policies and procedures to help meet its obligations under the Privacy Act and the Australian Government Agencies Privacy Code.

For the Census in particular, the ABS has developed a 'Privacy Strategy 2021-28' to ensure that privacy is considered across multiple Censuses, inclusive of the 2026 Census. The strategy sets out goals and focus areas of action to encourage ongoing improvement to management of personal information and to maintain community trust. The ABS also has a 2026 Census Security Strategy to ensure the security and privacy of Census data and a 2026 Census Data Protection Plan that sets out the principles, obligations, roles and responsibilities, and rules for the handling and protection of Census data and personal information required to operate the Census.

2 See ABS, 'Five Safes Framework.'

3 See OAIC, 'Privacy (Australian Government Agencies – Governance) APP Code 2017.'

Privacy for the 2026 Census is supported by the following roles:

- *Census Privacy Team* – Provides ongoing privacy support and awareness-raising within the 2026 Census Program; coordinates the Census Privacy work program; facilitates the PIA processes, including implementation of recommendations from PIAs and other review and assurance processes; works closely with the ABS Privacy Officer and Privacy Section to ensure consistency of messaging, advice and practice.
- *Census Privacy and Data Protection Working Group* – Provides advice on privacy matters, taking into account the importance of community participation and high-quality data for the Census. The Group is chaired by the General Manager Census and membership includes senior Census staff, the ABS Privacy Officer, ABS internal stakeholders and external representatives.
- *Census Data Protection Officer* – Role within the Census Privacy Team that helps to implement the Census Data Protection Plan, working in collaboration with Census data stewards and statistical managers.
- *Census Independent Privacy Advisor (CIPA)* – The CIPA has been engaged throughout the 2026 Census cycle to enhance privacy practices, identification of emerging risks and provides advice on privacy legislation. CIPA is a member of Census Privacy and Data Protection Working Group and regular meetings are held between Census Senior Executive to provide specialist privacy advice and discuss key privacy matters.
- *Security Operations Advisory Panel* – Oversees the security arrangements of Census systems, supported by the Technology and Security Division. This includes overseeing security assessments, compliance with security policies and procedures and other assurance processes. Additional Census fora also exist including the ICT for Census Governance Forum, CSD Technology Design Authority, Census 2026 Cyber Security Reporting Meeting and monthly security briefings with ABS's key technology partner.
- *Technology and Security Division* – Assists Census teams on the design and build of Census systems and information architecture while embedding security, in compliance with relevant security standards including the Protective Security Policy Framework (PSPF).

2.5 Approach to this PIA

The following sections outline IIS's approach to undertaking the PIA and analysing privacy issues. Being the third and final PIA of the 2026 Census, this PIA looked at the overall Census processes, but focused on addressing matters not covered in the Phase 1 and 2 PIAs, including matters identified by the ABS during internal PIA scoping.

Planning and topic prioritisation

IIS met with the ABS to discuss developments since the Phase 1 and 2 PIAs and the requirements for the Phase 3 PIA. The ABS Census Privacy Team developed a list of topics to be brought within the scope of the PIA and consulted the Census Privacy and Data Protection Working Group on the topics. IIS reviewed the topics and developed a PIA workplan setting out milestones and deliverables for the project. The topics prioritised for the Phase 3 Census are outlined in Section 2.2 above.

Information gathering

IIS held meetings with the relevant ABS Census teams to gather information about relevant aspects of the Census program, the associated information flows and the parties involved. This process was supplemented by IIS reviewing supporting documentation provided by the ABS to understand the key personal information data flows, controls and mitigations in place and, where relevant, progress since the Phase 2 PIA.

Stakeholder engagement

Engagement with stakeholders and community representatives is an important part of the PIA process. Consistent with the approach taken in the Phase 1 and 2 PIAs, IIS worked with the ABS to hold roundtable consultations with key stakeholders. Stakeholders invited to take part included privacy and advocacy groups, civil society groups, regulators, academics, researchers and data and ethics experts. The stakeholders were selected based on their:

- Representation of key sectors of Australian society
- Special interest or expertise
- Prior contribution to ABS PIA consultations.

See Appendix C for a list of stakeholders who took part in the Phase 3 consultation.

The objectives of the consultation process were to:

- Inform stakeholders about certain Census projects and proposals that the ABS is considering for the 2026 Census
- Seek stakeholder input on those projects and proposals.

To support the consultation, IIS prepared and distributed to stakeholders a short Issues Paper that provided background on the key topics in scope, along with questions for discussion. During June 2025 IIS held two virtual roundtable session with groups of stakeholders. IIS and the ABS also met independently with an individual stakeholder who could not attend with sessions. Stakeholders were able to offer feedback during the session and afterwards. They were also given the opportunity to provide a written submission.

The stakeholders provided valuable feedback which IIS took into account in the PIA analysis.

Preliminary findings and recommendations

IIS prepared an 'Outline of Draft PIA Recommendations' which was shared with the ABS for feedback on errors of fact. This involved IIS analysing the privacy issues taking into account feedback from stakeholder consultations. The ABS provided feedback on the draft recommendations which was taken into account in the drafting of this PIA report.

2.6 About this report

The Phase 1 PIA took a high-level, big picture approach to the privacy analysis, applying core privacy principles to identify risks and opportunities for best practice. The Phase 2 PIA engaged more closely with the specific requirements of the APPs and the Privacy Act. This PIA also focused on the requirements of the APPs and examined key areas which were not addressed in the previous two PIAs. IIS also evaluated the ABS's progress on recommendations made in those previous PIAs with the final evaluation provided to the ABS as a separate attachment.

The report is organised according to topic with each section offering a description of what is changing in relation to the topic followed by an analysis of data flows against key APPs. Each section concludes with a summary of the findings and, if applicable, a recommendation to address any identified gaps in compliance or privacy protection. Recommendations also identify opportunities for implementing best practice that goes beyond baseline compliance.

- *Executive summary* (Section 1) – including a summary of recommendations.
- *Introduction* (Section 2) – provides background on the PIA, its scope, the wider PIA context including the phased PIA approach, and the legislative framework.
- *Privacy analysis of key issues* (Section 3 to Section 9) – analyses key issues against the APPs and makes recommendations to mitigate risk and improve practice.
- *Glossary* (Appendix A).
- *Documents reviewed and meetings held* (Appendix B) – lists documents reviewed and meetings held as part of the information gathering process.
- *List of stakeholders* (Appendix C) – lists stakeholders who participated in roundtable consultations and/or who provided written submissions as part of the Phase 1 PIA process.

3. Sharing Census data via the DAT Act

Since the previous Census, the *Data Availability and Transparency Act 2022* (DAT Act) has come into force. Therefore, a possible change for the 2026 Census is that Census data may be the subject of data sharing requests under the DAT Act. The ABS has therefore been preparing for this possibility by considering how it would respond to any such request and how it would weigh the benefits and costs of sharing of Census data via the mechanism provided by the DAT Act.

The DAT Act establishes a data sharing scheme – the DATA Scheme – that allows agencies to share information for three permitted purposes: government service delivery; informing government policy and programs; and research and development. Its provisions override the secrecy provisions in other laws that might otherwise prevent data sharing. To address possible risks, the DAT Act establishes a range of protections that govern data sharing under the Act and restrict the purposes for which data may be used.

While there are already a number of ways that the ABS makes de-identified Census information available to researchers and others (DataLab, Census TableBuilder and other tools for access), the DAT Act creates an alternative legislative pathway to authorise the sharing of Australian Government data, including ABS-held Census data, with Accredited Users or Accredited Data Service Providers. Only accredited entities may receive information shared through the DAT Act and, in line with the *Privacy Act 1988*, personal information must be protected at all times.

3.1 Background

The sharing of Census data under the DAT Act was previously considered in the Phase 1 PIA and resulted in two recommendations that the ABS:

- Develop an internal decision-making process for considering and processing data sharing requests under the DAT Act (Phase 1, Recommendation 2)
- Conduct a risk benefit analysis in relation to sharing of historic Census data via the DAT Act (Phase 1, Recommendation 3).

The ABS has largely addressed these recommendations though IIS understands that the internal decision-making process is not yet operational, pending the outcome of the review of the DAT Act (which is ongoing at the time of writing).

The Phase 3 PIA is further assessing the possible sharing of future Census data under the DAT Act and the DATA Scheme it establishes. Note that IIS has conducted analysis based on the DAT Act in its current form and acknowledges that the recommendations below may require adjustment in line with any changes arising from the DAT Act review.

3.2 Personal and other information involved

This section of the PIA is concerned with Census information requested and shared under the DATA Scheme. The analysis focuses on sharing of future Census information (including information to be collected in the 2026 Census) and not historic Census information. Personal information involved includes data collected via Census forms and integrated into the Census dataset from other sources. Therefore, the information involved is:

- Statistical information – collected via Census forms.
- Administrative data – sourced from third party data custodians and integrated into the Census dataset post-Census 2026.

The data may be personal information and would be stored or shared in a de-identified form. Census data may be shared for DATA Scheme projects requiring integration with other datasets – in such cases, if linkage variables also need to be shared then standard data separation approaches would be strictly enforced.

Ensuring a consistent approach to ABS data sharing

During the information gathering phase of this PIA and in subsequent discussions, the ABS outlined the arrangements in place that govern data release at the ABS. This includes the application of the Five Safes Framework (closely aligned to the Data Sharing Principles in the DAT Act) to the release of ABS-held data and consideration by a Disclosure Review Committee to ensure the data is safe, appropriately de-identified, and being shared via a secure channel or platform.

The ABS noted that release of data under the DATA Scheme would likely follow existing data sharing arrangements including those that govern sharing of Census data via DataLab (and other existing channels) and those that govern sharing of PLIDA data – the Person Level Integrated Data Asset that the ABS hosts and manages. PLIDA is subject to a multifaceted governance framework applying both to the management of PLIDA and the sharing of PLIDA data for approved projects. The ABS explained that, for PLIDA, privacy risks were assessed and addressed at three levels:

- *System level* – Ensuring that privacy protections are applied to the technical infrastructure to ensure data integration, access, transmission and storage appropriately safeguard the data system.
- *Asset level* – Applying strong privacy settings for the PLIDA asset itself and ensuring responsible expansion of the data asset along with strong privacy governance.
- *Project level* – Examining research projects that wish to use PLIDA data on a case-by-case basis and ensuring that each project has appropriate ethical approvals, data minimisation, and risk mitigation strategies.

In addition, PIAs on PLIDA are conducted every two to three years and, for transparency, are published on the ABS's website.

As mentioned above, the ABS plans to use its existing arrangements for data sharing under the DATA Scheme, rather than introducing a new separate process that duplicates but deviates from existing processes. The idea is to leverage the strong privacy governance already in place rather than introduce inconsistency for DATA Scheme data sharing.

IIS has taken this into consideration in the discussion and analysis that follows.

3.3 Stakeholder feedback

Feedback provided during stakeholder consultations pointed out the importance of ethics consideration when sharing Census data under the DATA Scheme (and the risk that ethics committees may not have adequate privacy and technology related expertise). Stakeholders also drew attention to the potential risks of function creep due to the broad framing of DAT Act permitted purposes.

During the roundtables, stakeholders also discussed the possible heightened risk environment for data sharing due to the growing use and sophistication of AI technology (including a possible heightened risk of re-identification) and the need for strong re-identification risk management (including where additional categories of administrative data added to the Census dataset have the potential to increase re-identification risk).

Stakeholders emphasised the importance of transparency about DAT Act related data sharing and ongoing public trust (including the possible impact of loss of trust on Census participation).

3.4 APP analysis and other privacy risks

The DAT Act makes clear that the Privacy Act still applies to DAT Act data sharing. In its analysis, IIS found that the key APPs likely to apply to this form of data sharing are APPs 5 (Notice), 6 (Disclosure) and 11 (Security). By our analysis, and based on information provided by the ABS, we find that the ABS's current and proposed practices are likely to comply with APPs 5, 6 and 11. Further discussion of re-identification and AI-related risks is provided in Section 3.5 below.

IIS also considered key provisions of the DAT Act with possible relevance to privacy protection. In particular, IIS considered Data Sharing Principles under s 16 which include: the Project Principle, People Principle, Setting Principle, Data Principle and Output Principle. Note that IIS's review of DAT Act compliance was non-exhaustive and focused on key provisions relevant to the ABS's privacy arrangements vis-à-vis the DATA Scheme.

APP	*Comments and analysis*
Definition of PI	*Data shared under the DATA scheme and definition of personal information* The Privacy Act will only apply to data handling involving personal information. Whether Census information shared under the DATA Scheme is identified or de-identified will

APP	Comments and analysis
	depend on the project and the terms of the data sharing agreement. The ABS's Operating Principles for ABS participation in the DATA Scheme state that the ABS will not share personal information (or identified personal information) through the DATA Scheme, except with Australian Statistician approval. For reasons of best practice, IIS suggests the ABS follow key APPs regardless of whether the information is identified or de-identified to ensure a high level of privacy protection.
APP 5	*Notice of disclosure under the DATA Scheme* APP 5 requires an agency to inform an individual of certain matters when collecting their personal information. Under APP 5.2(f), this must include any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses the personal information in question. While the ABS cannot know ahead of time which Accredited Users may request Census data under the DATA Scheme, APP 5.2(f) makes clear that an agency should still indicate usual recipients of the information. The ABS informed IIS that it would be including information about possible disclosure under the DATA Scheme in its 2026 Census Privacy Statement. No further issues identified.
APP 6	*Disclosure of Census data under the DATA Scheme* APP 6 states that personal information must only be disclosed for the primary purpose it was collected unless an exception applies. Exceptions include where disclosure of the information is required or authorised by or under an Australian law (APP 6.2(b)). In this case, disclosure is authorised by the DAT Act. The ABS has developed (but not yet implemented) an internal decision-making process for considering requests for Census data which includes the participation of the ABS's Legal Team, among others – a step that will help ensure that a DATA Scheme project meets DAT Act requirements (and by extension the exception under APP 6.2(b)). Additional considerations regarding ethics and purpose limitation are discussed in Section 3.5 below. No further issues identified.
APP 11	*Safeguarding Census data shared under the DATA Scheme* APP 11.1 requires an agency to take reasonable steps to protect personal information against misuse, interference and loss, and from unauthorised access, modification or disclosure. In the case of the DATA Scheme, this obligation may apply both in terms of ensuring Census data is shared in a safe form (e.g. encrypted, de-identified etc) and ensuring the data is shared via a secure channel. These aspects of data security broadly align with the Data Principle and the Setting Principle contained in the DAT Act which are discussed further below.

APP	*Comments and analysis*
	The ABS has a range of information security arrangements in place to protect Census data, including when it is shared with researchers and others. For potential data sharing under the DATA Scheme, the ABS has a Risk Benefit Analysis Framework for assessing data requests which requires proactive identification and mitigation of risks. In addition, ABS advised that its IT systems (including those used for data integration and sharing) conform to the Information Security Manual (part of the Australian Government's Protective Security Policy Framework) and that systems are subject to a program of security audits and system accreditations. Re-identification risks associated with data sharing or data integration are proactively managed through data treatments and release via ABS-controlled environments with de-identification arrangements being reviewed by the ABS's Disclosure Review Committee (discussed further in the 'Data Principle' row below). Stakeholders raised concerns about the possible heightened risk environment introduced by AI technology. This is discussed further below in Section 3.5. Otherwise, the ABS appears to have strong security arrangements in place and strong risk identification arrangements (including the Risk Benefit Analysis Framework) for identifying project-specific risks. No further issues identified.
Provision	***DAT Act comments and analysis[4]***
Project Principle (public interest)	*Application of public interest test to DATA Scheme projects involving Census data* The Project Principle requires that a project must be reasonably expected to serve the public interest. The Data Availability and Transparency Code 2022 (DAT Code) gives further guidance on the application of this requirement and rules certain projects in the public interest including those serving the delivery of government services and those supporting medical research within the meaning given in the Privacy Act. For projects serving other purposes, the DAT Code prescribes matters that must be considered when weighing the public interest including any adverse impacts on individuals or groups of people, including impacts related to privacy, that can reasonably be expected to result from the project (cl 6(5)(a)(v)). The ABS advised that all data sharing by the ABS must follow the Five Safes Framework (which aligns closely with the DAT Act Data Sharing Principles). The Five Safes require that a project seeking ABS-held data demonstrate to the ABS that it has a public benefit. For PLIDA, new projects seeking access to PLIDA data are subject to a PTA (which

[4] IIS has conducted a high-level analysis of the application of the data sharing principles to the sharing of Census data, noting that specific DATA Scheme projects will raise additional specific issues that will call for more detailed analysis.

APP	Comments and analysis
	determines whether a PIA will be necessary). IIS understands a similar approach would apply to data sharing under the DATA Scheme. In addition, the ABS's Internal Decision-Making Process for DATA Scheme requests and the Risk Benefit Analysis Framework both provide for Legal Team review of requests to check the appropriateness of the proposed data sharing. The Risk Benefit Analysis Framework also specifies that documented legal advice from the Legal team must confirm that it has not identified any legal restriction to sharing the data identified. IIS understands that public interest considerations would be considered during this stage of the ABS's internal processes to ensure compliance with the Project Principle. It appears from these arrangements that the ABS has adequate measures in place to meet public interest requirements on a case-by-case basis. No further issues identified.
Project Principle (ethics)	*Application of ethics requirements to DATA Scheme projects involving Census data* The Project Principle requires that parties observe processes relating to ethics, as appropriate in the circumstances. The DAT Code gives further guidance on the application of this requirement including clarifying that appropriate ethics processes may include no ethics process. The DAT Code also notes that applicable ethics processes may be a matter of law or policy and that where more than one ethics process applies, only one ethics process need be observed to meet the ethics requirement in the Project Principle. Finally, the DAT Code clarifies that the Project Principle does not require entities to observe any ethics processes additional to those otherwise applicable but does not prevent entities from observing additional ethics processes if they wish. The ABS advised that the same ethics arrangements in place for PLIDA would apply to data sharing under the DATA Scheme. That is, all projects, as part of standard PLIDA governance processes, would be asked to confirm if they have sought or received ethics approval for the project and copies of ethics documentation would be provided to the ABS. Additionally, the ABS's Internal Decision-Making Process for DATA Scheme requests and the Risk Benefit Analysis Framework both provide for Legal Team review of requests to check the appropriateness of the proposed data sharing. The Risk Benefit Analysis Framework also specifies that documented legal advice from the Legal team must confirm that it has not identified any legal restriction to sharing the data identified. IIS understands that applicable ethics processes would be checked during this stage of the ABS's internal processes (including what (if any) applicable ethics processes may apply). From these arrangements it appears the ABS has adequate measures in place to meet DAT Act ethics requirements. Further discussion of ethics is below – see Section 3.5.

APP	Comments and analysis
People Principle	*Application of the People Principle to DATA Scheme projects involving Census data* Under the DAT Act, the People Principle is that data be made available only to appropriate persons. IIS has not reviewed the application of the People Principle in detail as its application will depend on the nature and circumstances of each DATA Scheme project. However, the ABS's standard processes, in line with the Five Safes Framework, generally require data recipients to sign a legally binding undertaking to maintain data confidentiality and to receive training in confidentiality and conditions applying to data use. IIS also notes the ABS's policy (set out in the Operating Principles) of sharing data via an ABS administered and controlled secure environment in preference to the IT environments of other Accredited Users or Accredited Data Service Providers (see Setting Principle below). This gives the ABS robust access control over data access by Accredited Users, along with strong oversight of user access and activity. IIS understands that specific access arrangements would be determined in line with any Data Sharing Agreement, in compliance with the requirements set out in the DAT Act and the DAT Code. No further issues identified.
Setting Principle	*Application of the Setting Principle to DATA Scheme projects involving Census data* Under the DAT Act, the Setting Principle is that data is shared, collected and used in an appropriately controlled environment. The ABS's Operating Principles for participation in the DATA Scheme include the principle that the ABS will provide access to data in an ABS administered and controlled secure environment in preference to the IT environments of other Accredited Users or Accredited Data Service Providers. IIS understands that this could include making data available via the ABS-owned and managed 'Secure Environment for Analysing Data' (SEAD) which has been designed to embed DAT Act Data Sharing Principles and meet the requirements of the Setting Principle. The Australia National Data Integration Infrastructure (ANDII) is another ABS-owned and managed platform which currently hosts the National Disability Data Asset (NDDA). Both SEAD and ANDII have been subject to privacy and security testing. The ABS appears to have appropriate infrastructure in place to meet the Setting Principle. This coupled with a policy of preferring ABS IT environments over third party systems is likely to ensure a strong setting for data sharing. No further issues identified.

APP	Comments and analysis
Data Principle	*Application of the Data Principle to DATA Scheme projects involving Census data* Under the DAT Act, the Data Principle requires that appropriate protections be applied to data to be shared under the DATA Scheme and that only the data reasonably necessary to achieve the data sharing purpose is shared. What protections will be appropriate will depend on the circumstances, and the ABS has made clear in its Operating Principles that it will consider DATA Scheme requests on a case-by-case basis. IIS also understands that a Risk Benefit Analysis will be conducted for each DATA Scheme project to further support case-by-case consideration of project scope, benefits, risks and controls. Due to its other data sharing activities, the ABS has well-established de-identification arrangements in place. The ABS applies the Five Safes Framework to proposed data sharing to ensure data is disclosed in a manner that is unlikely to enable identification of an individual within the data. As part of meeting the 'Safe Data' element of the Five Safes (equivalent to the Data Principle in the DAT Act), the ABS conducts a Safe Data Assessment. In conducting the assessment, the ABS employs criteria and a risk assessment matrix to determine whether the data is low, medium or high risk, from a re-identifiability standpoint. All medium and high risk data (and accompanying Safe Data Assessments) must be reviewed by the ABS's Disclosure Review Committee. (IIS understands that Census data automatically triggers Disclosure Review Committee review.) The ABS advised that the Disclosure Review Committee's terms of reference had been expanded to include provision of advice relating to ABS participation in the DATA Scheme in the area of Safe Data and Safe Data Assessments. De-identification techniques employed by the ABS include both baseline de-identification such as the removal of direct identifiers and additional data treatments depending on the release context such as limiting the number of variables, modifying cell values, combining categories, collapsing top or bottom categories containing small populations, data swapping, and cell suppression.[5] From these arrangements, IIS finds that the ABS has strong de-identification measures in place to meet Data Principle requirements. Further discussion of re-identification risk is below – see Section 3.5.
Output Principle	*Application of the Output Principle to DATA Scheme projects involving Census data* The Output Principle regulates the form of a project's final output and the data it may contain. IIS has not reviewed the application of the Output Principle in detail as its application will depend on the nature and circumstances of each DATA Scheme project. Discussion of the Setting Principle above notes that the ABS will usually share data under the DATA Scheme via an ABS administered and controlled secure environment in

[5] For more information about de-identification techniques, see the *Treating microdata* page of the ABS's website.

APP	Comments and analysis
	preference to the IT environments of an Accredited User. This will provide a higher level of ABS control over any statistical output created from Census data shared under the DATA Scheme, including ensuring that such outputs are non-disclosive. Disclosure risks associated with a project output would, IIS understands, be considered via the ABS's Risk Benefit Analysis Framework and under a dedicated Safe Data Assessment. No further issues identified.

3.5 Further discussion and recommendations

Overall, IIS finds that the ABS has strong internal governance arrangements in place to manage data sharing. In the discussion below, we address matters that were raised by stakeholders or that warrant careful assessment, in light of privacy risk or sensitivity.

Ethics consideration for DATA Scheme projects

Per the analysis contained in the table above (regarding the Project Principle), IIS finds that the ABS has measures in place that support DAT Act ethics compliance. However, given the particular risk profile of Census data,[6] IIS gave special consideration to ethics arrangements governing DATA Scheme data sharing. In particular, IIS considered the fact that the DAT Act allows for no ethics consideration in some circumstances. In discussing this possible gap in ethics consideration with the ABS, the ABS explained that it took a risk-based approach to assessing data sharing proposals and to assessing whether ethics consideration was needed. The ABS advised IIS that its preference was to follow the process already in place for PLIDA.

It is relevant to note that a recent PLIDA PIA recommended that that the ABS consider further strengthening the ethics approval arrangements for PLIDA by developing a PLIDA Ethics Framework to provide a systematic process for considering the ethical use of PLIDA datasets containing Health Data, to assist researchers and stakeholders understand the potential ethical issues.[7] In its response to the PIA, the PLIDA Board acknowledged that a PLIDA Ethics Framework would help to standardise decisions about data use and transparency and agreed to develop a framework for the use of PLIDA datasets, including those containing Health Data.[8] IIS understands that work on the Framework is underway and draws on the APS Data Ethics Framework, as well as Data Ethics Frameworks of other National Statistical Offices. The framework will address both the PLIDA PIA recommendation as well as the data ethics recommendation from the Phase 2 PIA.

---

6 That risk profile includes: the breadth of the dataset (population-wide), the richness of the dataset, and the impact of a loss of trust or social acceptance on participation in the Census.

7 See Recommendation 3, PIA on *Expanded Health Data Linkage to the Person Level Integrated Data Asset (PLIDA)*, 23 May 2024.

8 See PLIDA Board Response to the PIA on *Expanded Health Data Linkage to the Person Level Integrated Data Asset (PLIDA)*, 23 May 2024.

The ABS indicated a preference for using existing governance arrangements for DATA Scheme data sharing, where possible – including existing PLIDA arrangements. This would seem to indicate that the ABS would also apply a similar process for ethics consideration which, in accordance with the recent PLIDA PIA recommendation outlined above, would occur in line with a soon-to-be-implemented PLIDA Ethics Framework. We therefore recommend that the ABS consider whether the PLIDA Ethics Framework might be effectively adapted for use in DATA Scheme data sharing also. In addition, to ensure strong assurance and oversight, we recommend that a decision to proceed with Census data sharing under the DATA Scheme, in which no ethics process has taken place, require endorsement at a suitably senior level within the agency. See Recommendation 1.

Recommendation 1 – Ensure consistent ethics arrangements for any DATA Scheme projects involving Census data sharing.

Best practice

1.1 Consider adapting the forthcoming PLIDA Ethics Framework for use in DATA Scheme data sharing also. The purpose of this recommendation is to encourage a consistent, rigorous and systematic approach to ethics consideration at the ABS as it applies to data release and data sharing projects. Note that this is a best practice recommendation – analysis conducted in this PIA indicated that the ABS has arrangements in place that would allow it to meet DAT Act ethics requirements on a case-by-case basis.

Best practice

1.2 Require senior endorsement of a decision to proceed with data sharing for a DATA Scheme project for which no ethics process has taken place. 'Senior endorsement' means endorsement by an appropriately senior employee of the ABS. Ensure internal policies and procedures document the position of the senior employee who must endorse the decision.

The DAT Act permits no ethics process in some circumstances. The purpose of this recommendation is to ensure that a decision to go ahead with a DATA Scheme project that has not been subject to ethics consideration is subject to appropriate assurance and oversight at a senior level of the agency.

Purpose limitation

Comments during the roundtable discussion drew attention to the broad framing of the permitted purposes in the DAT Act and the risk of function creep and associated risk of community loss of trust.

In considering this matter, IIS reviewed the ABS's DAT Act governance arrangements which include a set of Operating Principles for ABS participation in the DATA scheme (Operating Principles), an internal decision-making process for Census DATA requests and a Risk Benefit Analysis Framework which can be used to assess requests under the DAT Act. In reviewing these documents, IIS observed that

Operating Principle 2 specifies that 'The ABS will only consider entering into DATA Scheme data sharing agreements that are consistent with the functions of the ABS set out in the ABS Act, and consistent with the ABS purpose, its role and its priorities.' Additionally, the Risk Benefit Analysis Framework requires clarification, definition and endorsement of project scope along with assurance that the project scope aligns with ABS objectives. The DAT Act further requires a data sharing agreement made under the Act to describe the project and the data sharing purpose. The agreement must also describe how the public interest is served by the project and the permitted final output.

IIS finds that these mandatory features of a DATA Scheme data sharing agreement, along with the ABS's internal processes requiring clarification, definition and endorsement of project scope during the Risk Benefit Analysis demonstrate appropriate steps to embed a principle of purpose limitation and hence minimise function creep. We encourage the ABS to define project purpose in adequate detail to limit unintended secondary uses. No further issues were identified.

De-identification

At various points, stakeholders raised concerns about re-identification risks in relation to Census data sharing (particularly instances of heightened risk introduced by the impact of AI technology or by inclusion of administrative data). The ABS already employs a range of techniques in de-identifying Census data when making it available through existing channels (such as Data Lab and Tablebuilder). The question, therefore, is whether those techniques and processes continue to be fit for purpose as the risk environment evolves.

IIS reviewed ABS systems and processes and found that the ABS has strong de-identification arrangements in place. This is evident in the analysis in the table above checking ABS compliance with the Data Principle in the DAT Act. But an evolving risk environment also calls for measures that ensure rigorous case-by-case assessment of risk, including re-identification risk. IIS reviewed the measures in place and found that the ABS takes a risk-based approach to data sharing based on defined criteria which allows for a nuanced approach to managing de-identification with escalation points and additional oversight for higher risk data. Central to the ABS's de-identification measures are the Safe Data Assessments, completed for each proposed data release, and Disclosure Review Committee review, both of which allow case-by-case consideration of data treatments.

Case-by-case consideration is one of the ABS's DATA Scheme Operating Principles. Other lines of defence include applying the other four 'Safes' and use of the Risk Benefit Analysis Framework. For DATA Scheme projects involving the creation of enduring integrated data assets, IIS understands that the ABS's usual practice is to develop a De-identification Strategy – as occurred in the cases of the NDDA and PLIDA.

Stakeholder concern regarding re-identification risk is understandable – it is for that reason IIS has taken care to thoroughly review de-identification measures – and it is our view that the ABS has measures in place to ensure safe data sharing in an evolving risk environment. During preliminary analysis, IIS considered whether further measures might be necessary. On reviewing the ABS's systems and

processes, we are satisfied that the ABS is managing re-identification risk effectively – including in cases where the data context changes due to data sharing.

AI related risk associated with Census data sharing

IIS recommends the ABS take steps to ensure AI-related risk associated with sharing of Census data is proactively addressed – see Recommendation 2. While all advances in technology may pose privacy risks, IIS finds that the rapid acceleration of AI technology calls for particular care to ensure ongoing safe data processing. Comments made by stakeholders included concerns over risks posed by AI particularly in any cases where Census data moves outside ABS control. Those risks included heightened risks of re-identification using AI tools and possible use of Census data to train AI and Large Language Models (LLMs). In addition to the recommendation below, IIS suggests that the ABS maintain a watching brief on developments in AI technology (if it does not do so already) to foster up-to-date awareness of and knowledge about possible emerging risks.

It is worth noting that the ABS has taken steps recently to enhance the transparency of its use of AI and related technologies by publishing information on its website. IIS understands that that information will be updated as necessary to reflect new or different uses of AI technology by the ABS, including use in DATA Scheme projects. IIS also understands that the ABS will continue to publish the privacy, security and assurance arrangements in place for its AI use. We therefore find the ABS is taking appropriate steps to ensure ongoing transparency of its activities in these areas.

Recommendation 2 – Ensure careful management of AI-related risks associated with any Census data sharing

Compliance

2.1 Update relevant internal policies and procedures to ensure AI-related risks and controls are identified and addressed in relation to Census data sharing (including, but not limited to, sharing under the DATA Scheme). AI-related risks may include a heightened risk of re-identification, unintended secondary use or disclosure (including disclosure to third party systems or systems outside Australia), and/or negative publicity.

In addressing this recommendation, the ABS could consider making assessment of AI-related risk a standing item in the Risk Benefit Analysis Framework template and/or the PTA template. For the avoidance of doubt, this recommendation does not intend to prohibit appropriate use of AI technology in connection with Census data sharing. In this recommendation, AI includes Machine Learning (ML) and Large Language Models (LLMs). It goes to compliance with APP 11.1 and taking reasonable steps to safeguard personal information.

Transparency of DATA Scheme data sharing

Stakeholders raised the importance of transparency about DATA scheme sharing to ensure ongoing public trust and social acceptance. The ABS has provided information on the steps it is taking to ensure transparency of its data sharing activities under the DATA scheme. This includes a webpage with information, inclusion of DATA scheme information in the 2026 Census Privacy Statement, inclusion of DATA scheme projects on the Office of the National Data Commissioner website and inclusion of (summarised) data sharing agreements on a public register.

IIS finds the ABS is taking reasonable steps to ensure transparency of its activities under the DATA scheme, including meeting its obligations under APP 5. We encourage the ABS to continue to look for opportunities to raise awareness about these activities. No further issues were identified.

4. Enhancing the Census dataset with administrative data

The ABS is proposing to use certain categories of administrative data to enhance the 2026 Census dataset. Using administrative data to enhance the Census dataset was raised with stakeholders during consultations for the Phase 2 PIA. It was 'Use Case 3' of three administrative data proposals. During the Phase 2 PIA, it was decided that Use Case 3 would be held over and addressed during the Phase 3 PIA when there was further certainty about the variables proposed to be added to the Census dataset.

4.1 Changes expected in 2026

In 2026, the ABS proposes to use administrative data to enhance the Census dataset. Administrative data was added to the 2021 Census dataset to enhance income data and improve its accuracy. For the 2026 Census, the ABS is proposing adding the same income-related administrative data along with some additional income variables as well as administrative data on vehicle ownership and solar panel installation.

The ABS advised that the addition of administrative data to successive Census datasets would continue to be limited. Other data assets, such as the Person-Level Integrated Data Asset (PLIDA), already contain integrated administrative datasets from a wide range of sources which make their secondary inclusion in the Census dataset unnecessary. The ABS has advised that the main reason for inclusion of certain additional variables sourced from administrative data is to improve the accuracy of Census data, add some higher definition to existing questions and, in future Censuses, reduce the respondent burden of filling out the Census form (e.g. by removing the existing income and motor vehicle questions).

4.2 Personal and other information involved

The ABS proposes adding person-level and dwelling-level variables sourced from administrative data. The data would be de-identified but imported with linkage information to enable linkage with the Census dataset. Proposed variables include:

- Income (including individual and household income and total income five years ago)
- Main source of income
- Main government benefit (including length of time received)
- Rent assistance (including amount and length of time received)
- Mortgage affordability indicator and rent affordability indictor
- Number of vehicles of a household
- Vehicle type and fuel type
- Solar panel installation.

Income-related administrative data and administrative data about government benefits will be sourced from PLIDA while vehicle information and solar panel information will be sourced from third party data custodians.

4.3 Stakeholder feedback

Stakeholders offered varied views on the use of administrative data to enhance the Census dataset with some considering that integration of administrative and Census data should be strictly limited while others noted the value of income, motor vehicle and solar panel data to researchers. Those urging caution encouraged the ABS to take an incremental approach to expanding the types of administrative data integrated into the Census (in line with Phase 1, Recommendation 8) and noted the risk of a loss of trust if the ABS moves too quickly. Others pointed out that there was particular benefit to researchers to be able to access national data for those datasets normally stored by state (such as motor vehicle data).

Stakeholders discussed the relative sensitivity of the proposed administrative datasets. Some felt that motor vehicle and solar panel data was fairly 'non-sensitive' but thought that income data could be considered more sensitive – particularly if individuals have concerns about cross-referencing of income data to allow enforcement action (e.g. in cases of under-reported income). In addition to this, there was some discussion about whether the level of granularity of the data may be a risk for these administrative data variables if it allows unintended re-identification.

IIS also received feedback about use of administrative data without an individual's consent and the potential risk of creating a perception of government surveillance (whether true or not), particularly within marginalised social and cultural groups who have been harmed by government actions (such as First Nations people and individuals impacted by Robodebt). It was also noted that the risk of mistrust may be higher in situations where the data custodian for the administrative data is an organisation that an individual has not heard of or would not expect to be holding their information.

As with other matters raised in this PIA, stakeholders emphasised the importance of transparency and suggested the ABS work with administrative data custodians to check the efficacy of initial privacy notices.

4.4 APP analysis and other privacy risks

IIS assessed this administrative data use case against the requirements of the Privacy Act. In particular, IIS considered the application of APPs 3.1 (Collection), 3.5 (Fair and lawful collection), 3.6 (Direct collection), 5 (Notice), 6 (Use and disclosure), and 11 (Data security).

APP	Comments and analysis
Definition of PI	*Is the administrative data personal information?* The Privacy Act and APPs only apply to 'personal information' which is defined in the Act as information or an opinion about an identified individual or an individual who is reasonably identifiable. Therefore, a threshold question is whether the data in question is personal information. The ABS has advised that administrative data will be imported into an ABS environment following data separation principles. That is, linkage variables (such as name, address etc in coded and hashed form) are imported separately to the analytic variables (such as income information, vehicle ownership etc) and no single person is able to see or access both at once. It is clear the ABS has strong data separation and de-identification arrangements in place (as discussed in Section 3). That said, given the breadth and richness of the data and the possible privacy impact of misuse, IIS recommends treating the data as if it were personal information and applying the principles accordingly.
APP 3.1	*Collection of administrative data about vehicle ownership and solar panels* APP 3 states that an agency must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the agency's functions or activities. The ABS is collecting this administrative data to enhance the Census dataset and improve the statistics available about the Australian population. This is directly related to the ABS's functions and activities as set out in the ABS Act and the Census and Statistics Act. Moreover, collection is also likely to be permitted by APP 3.4(a) which permits collection where it is required or authorised by an Australian law – in this case, the Census and Statistics Act. In assessing the application of APP 3, IIS has focused on the ABS's collection of vehicle and solar panel administrative data which the ABS proposes to collect for this use case. Income related administrative data would be sourced from PLIDA which is already held and managed by the ABS. This means that, although the ABS must follow certain procedures to access that data and 'collect' it into its Secure Data Integration Environment to enable integration with the Census dataset, that is technically treated as a 'use' under the Privacy Act rather than a collection. Therefore, access to, and use of, income-related administrative data is regulated by APP 6 (use) rather than APP 3. No further issues identified.
APP 3.5	*Collection of administrative data is fair and lawful* APP 3.5 requires that an agency only collect personal information by fair and lawful means. IIS finds that the ABS's collection of administrative data for this use case meets the lawful limb of this principle. Regarding fairness, the OAIC advises that a 'fair means' of

APP	Comments and analysis
	collecting information is one that does not involve intimidation or deception, and is not unreasonably intrusive.' The OAIC further advises that, depending on the circumstances, 'it would usually be unfair to collect personal information covertly without the knowledge of the individual.'[9] The ABS has no intention of hiding its collection and use of administrative data. That said, its challenge is to ensure its collection and use is overt and clear to the public in circumstances where the public may not otherwise be aware of the collection, given that the collection occurs indirectly and involves data that was originally collected for an unconnected purpose. IIS understands that the ABS is taking and has taken steps to research community attitudes to administrative data use and research the most effective ways to raise awareness about administrative data use. We understand that that research has informed a communications strategy on this issue. In response to APP 5 and stakeholder feedback, IIS is also recommending that the ABS work with data custodians where possible to ensure initial privacy collection notices mention collection by the ABS (see APP 5 discussion below). No further issues identified.
APP 3.6	*Collection of administrative data from sources other than the individual* APP 3.6 requires an agency to collect personal information directly from the individual unless an exception applies. Exceptions include where the individual consents to indirect collection; where the agency is required or authorised by law to collect the information indirectly; or where direct collection would be unreasonable or impracticable. IIS finds that the ABS's collection of administrative data from data custodians is likely to meet the 'authorised by law' exception. That said, IIS notes that, in response to recommendations made in earlier phases of the PIA, the ABS is taking and has taken steps to improve awareness about administrative data use, including development and deployment of a communications strategy on the issue. Transparency is particularly important in cases where personal information is collected indirectly. No further issues identified.
APP 5	*Privacy notice obligations in relation to administrative data use* APP 5 requires the ABS to take reasonable steps to make individuals aware of certain matters (set out in APP 5.2) when collecting personal information. Those notice obligations apply regardless of whether the collection is direct or indirect. The Phase 2 Census PIA recommended the ABS include information about administrative data collection in the Census 2026 Privacy Statement (see Phase 2, Recommendation 4) – a recommendation the ABS accepted and is on track to complete. In this PIA we are also recommending the

[9] OAIC, APP Guidelines, paragraph 3.62

APP	*Comments and analysis*
	ABS work with data custodians to encourage inclusion of relevant information in their respective privacy collection notices. Some additional transparency considerations are discussed in Section 4.5 below. See **Recommendation 3**.
APP 6	*Use of administrative data to enhance the Census dataset* The ABS will use administrative data about income, vehicle ownership and solar panel installation to improve the accuracy of Census data, add some higher definition to existing questions and, in future Censuses, reduce the respondent burden of filling out the Census form (e.g. by removing the existing income and motor vehicle questions). This will involve importing administrative data (from third party data custodians and from PLIDA) and integrating that data with the Census dataset. Data linkage would be done following data separation principles and would take place in a secure data linkage environment. APP 6 states that personal information must only be used for the primary purpose it was collected unless an exception applies. IIS finds that, with regards to vehicle and solar panel data, the proposed data processing outlined above falls within the primary purpose of collection and therefore meets APP 6. For income data already held by the ABS in PLIDA, use of the data to enhance the Census dataset could be considered a 'primary purpose' given that the data is collected into PLIDA for use in approved research projects, of which this use case is one. If use of PLIDA-sourced income data for this use case is treated as a 'secondary purpose,' that use is likely to meet the exception in APP 6 allowing a secondary use authorised by law – with the authorising legislation in this case being the Census and Statistics Act. The Act permits the ABS to undertake surveys and the Census, collect information from other data custodians and link Census data and other information. IIS also notes that PLIDA is subject to its own governance arrangements which include a rigorous assessment and approval process for projects wishing to use PLIDA data. For a project to be approved the data custodians must agree to the proposed use of the data and the project must be assessed as being in the public interest.[10] No further issues identified.

[10] See ABS, PLIDA/MADIP research projects.

APP	Comments and analysis
APP 11	*Security arrangements for Census data and administrative data* APP 11 requires an agency to take reasonable steps to protect the personal information it holds from misuse, interference and loss and from unauthorised access, modification or disclosure. The ABS already has well-established systems in place to bring administrative data into the agency in a safe and secure way. IIS understands that this would involve use of an accredited secure transfer method (to be agreed with respective data custodians) and that data separation principles would apply. In practice, this means that linkage variables and analytical variables are kept separate and that data access is role-restricted with no ABS officer having a complete view of the dataset at any time. IIS understands that the ABS was still to determine where data linkage (of Census data and administrative data) would take place but that it was possible that it would be via a Secure Data Integration Environment such as the SEAD or the ANDII environments – both of which have been subject to rigorous privacy and security testing. Once administrative data has been integrated with the Census dataset, the ABS will apply the Five Safes Framework. As part of that process, the ABS would conduct a Safe Data Assessment to check de-identification arrangements and then submit the dataset for review by the Disclosure Review Committee. These measures are applied prior to any data being made available to researchers (via DataLab for example). Further information about the ABS's de-identification process is provided in Section 3. More broadly, IIS understands that the security arrangements of Census systems are overseen by the ABS's Security Operations Advisory Panel, supported by the Technology and Security Division. Systems handling Census data are accredited to the PROTECTED level, based on the Protective Security Policy Framework (PSPF) and are Infosec Registered Assessors Program (IRAP) assessed. All systems involved in Census-related data processing are access restricted following the principle of least privilege. A security assessment was out of scope for this PIA. However, the overarching security measures in place, both for Census generally and for administrative data processing in particular indicate that the ABS is taking reasonable steps to safeguard the personal information it holds. No further issues identified.

4.5 Summary and recommendations

Following our analysis of the issues under the APPs and consideration of other privacy risks, IIS makes two recommendations to strengthen privacy arrangements.

APP 5 compliance

IIS assessed this administrative data use case against the requirements of the Privacy Act. We find that the ABS's proposed activities are likely to meet the requirements of the APPs though suggest the ABS work with administrative data custodians to ensure adequate notice at the initial point of collection of personal information in accordance with APP 5 (see Recommendation 3).

Recommendation 3 – Work with administrative data custodians so that initial collection notices make clear the disclosure of data to the ABS

Compliance

3.1 Work with administrative data custodians to encourage them to review and update (as reasonable in the circumstances) relevant collection notices to make clear the disclosure of data to the ABS. This will be particularly important in relation to data custodians from whom the ABS has not previously collected administrative data where notice arrangements may not already be in place. The purpose of this recommendation is to meet the requirements of APP 5 to take reasonable steps to make individuals aware of the collection of personal information by the ABS.

Incremental approach to administrative data use and decisions about expansions to use

While some stakeholders saw value in the addition of administrative data to the Census dataset, some concern was also expressed about 'moving too fast,' the importance of taking an incremental approach, and the risk of loss of trust and social acceptance. These concerns relate to matters beyond the requirements of privacy law to questions of 'what is appropriate?' and 'can versus should' and 'how much administrative data use is too much?' Such questions are questions the ABS will continue to face in successive Censuses as it adjusts or expands its administrative data activities. IIS finds they are best addressed via the data ethics process recommended under the Phase 2 PIA, Recommendation 8.

Community understanding of administrative data use and addressing concerns

In response to Phase 1 PIA recommendations, the ABS has researched effective communications methods for increasing understanding of administrative data use and developed a communications plan. During consultations with stakeholders, there was some concern about use of administrative data (particularly income data) for enforcement purposes. One roundtable participant also asked whether third party sourced administrative data would be included with Census form data for release by the National Archives of Australia where an individual opts for their Census information to be made public in 99 years – the participant suggested the ABS clarify this.

IIS acknowledges stakeholder feedback, including in relation to marginal groups and ensuring trust and understanding about administrative data use. We find that actions taken in response to Recommendation 8 in the Phase 1 PIA and Recommendation 5 in the Phase 2 PIA have put the ABS in a strong position to understand community sentiment and communicate effectively to address concerns. In addition, IIS

suggests the ABS publicly address the particular questions and concerns raised by stakeholders, outlined in Recommendation 4 below.

Recommendation 4 – Publicly address questions about administrative data use and disclosure (including clarity on restrictions involving disclosure to the National Archives of Australia and restrictions on use for enforcement)
Best practice 4.1 Clarify (in the 2026 Census privacy notice and/or other relevant communications material about administrative data use in the Census) whether administrative data about an individual is released to the National Archives of Australia in the event that the individual opts to allow their Census form to be made public after 99 years. The purpose of this recommendation is to ensure transparency about how Census data (including administrative data) is used, disclosed and published.
Best practice 4.2 Make clear (in the 2026 Census privacy notice and/or other relevant communications material about administrative data use in the Census) that the ABS does not use administrative data for enforcement or compliance activities. Clarifying information may be particularly important for income-related administrative data.

Re-identification risks

Stakeholders suggested that there may be a heightened re-identification risk for the Census dataset in adding in the proposed additional administrative data variables.

IIS finds that the ABS has adequate de-identification arrangements in place to manage re-identification risks including new risks posed by additional variables. All sharing of Census data occurs in line with the Five Safes Framework, of which the Data, Settings and Output 'Safes' go to ensuring strong de-identification settings. The ABS uses a range of de-identification techniques. This includes both baseline de-identification such as the removal of direct identifiers and additional data treatments depending on the release context such as limiting the number of variables, modifying cell values, combining categories, collapsing top or bottom categories containing small populations, data swapping, and cell suppression. The ABS advised that release of Census data is always subject to a Safe Data Assessment and review by the ABS's Disclosure Review Committee prior to release.

No further issues were identified.

5. Separate forms within a single household

An issue identified for consideration in this PIA was the matter of enabling separate forms from within a single household to offer further privacy to individuals filling out the Census.

5.1 Background

Following the Government's decision to include a new topic of 'sexual orientation and gender' for people aged 16 years and older, the ABS plans to introduce two new questions to the 2026 Census on gender and sexual orientation. In recognition of the potential sensitivity of these questions, the ABS will offer a 'prefer not to say' response option for both questions. An additional option is for individuals within a household to request a separate form to fill out, rather than having their responses included in a household form with other household members.

IIS understands that it has been possible for individuals to complete a separate Census form in previous Censuses with the ABS reconciling and merging forms for a household during data processing. Similarly in the 2026 Census, individuals will be able to access a separate household form through the Census website or by calling the Census Contact Centre. The ABS indicated that it is also exploring the option of providing a personal form through the Census Contact Centre. A personal form contains the same questions as in the household form but excludes dwelling related questions and is for one individual only.

5.2 Personal and other information involved

This issue relates to the means of collection of Census forms. Therefore, the personal information involved is statistical information – collected via Census forms.

5.3 Stakeholder feedback

Generally, participants in the roundtables supported the option of allowing separate Census forms within a single household. However, there was some discussion about how the option of separate forms would work in practice. For example, would an individual have to tell a person filling out a household form that they would like to fill out a separate form and how would the ABS manage cases where the household form includes information about an individual who has also filled out a separate form. It was noted that seeking a separate form might, in and of itself, provoke unwanted questions for an individual about their reason for wishing to use a separate form.

Stakeholders also asked whether a person filling out either a household form or separate form might be penalised for submitting incorrect information where the household form and separate form contain inconsistent information about a single individual. One stakeholder also pointed out that if the ABS linked the inclusion of questions relating to gender and sexual orientation to the reason why a separate form is available, the very fact that an individual may choose to complete a separate form may, in and of itself, reveal personal and sensitive information about that person (whether true, or not), to those who find out that a separate form has been used.

5.4 APP analysis and other privacy risks

This issue relates to the 'collection' stage of the information lifecycle. Therefore, the APP analysis below focuses on the application of APP 3 (Collection) – in particular, APP 3.5 (Collection must be fair and lawful), APP 3.6 (Collection must be direct from the individual unless an exception applies) and APP 10 (Data quality).

APP	*Comments and analysis*
APP 3.5	*Collection only by fair and lawful means* APP 3.5 states that an agency must collect personal information only by lawful and fair means. Of relevance to the issue under consideration is the fairness limb of this APP. The OAIC advises that a 'fair means' of collecting information is one that does not involve intimidation or deception, and is not unreasonably intrusive.[11] It's possible that for some individuals, collection of statistical information about them via a household form may be unreasonably intrusive if it means personal information, that they prefer to keep private, is disclosed to other members of the household during form filling. This form of privacy risk may be heightened in 2026 due to the inclusion of questions on gender and sexuality which may be sensitive for some people. While many are likely to be comfortable filling out a household form as they have done in years past, it seems reasonable to ensure individuals are able to access a separate form if they wish. This would strengthen the 'fairness' of collection per APP 3.5 and reduce the likelihood of privacy intrusion during collection. As noted above, it has been possible for individuals to complete a separate Census form in previous Censuses, so the key issue is about how this option is promoted to individuals. See **Recommendation 5**.
APP 3.6	*Collection direct from the individual* APP 3.6 requires an agency to collect personal information directly from the individual unless an exception applies. Exceptions include where the individual consents to indirect collection; where the agency is required or authorised by law to collect the information indirectly; or where direct collection would be unreasonable or impracticable. Generally, collection of information via Census forms would be considered a 'direct' collection, notwithstanding that one member of the household may fill in responses for others in the house on Census night. Requiring each individual to fill out their own form to ensure collection is 'direct' would be unreasonable and impracticable. In our view, existing arrangements meet APP 3.6. That said, ensuring individuals are able to access a separate form if they wish would assist the ABS in meeting the spirit of APP 3.6 by offering a more direct means of collection.

[11] OAIC, *APP Guidelines*, Part 3, paragraph 3.62.

APP	*Comments and analysis*
	No further issues identified.
APP 10	*Quality of personal information* APP 10.1 states that an agency must take reasonable steps to ensure that the personal information it collects is accurate. The intended use of Census information for statistical purposes is relevant to the interpretation of this principle. Given that there is no direct impact on the individual regarding inaccurate Census information, the privacy impact is significantly reduced. So, the steps that are 'reasonable' for the purposes of APP 10 might be lesser than in a case where inaccurate information may have a direct, adverse impact on an individual. IIS finds, therefore, that steps to ensure data accuracy will be driven by statistical objectives (i.e. ensuring data used in the production of statistics is accurate) rather than privacy ones (i.e. ensuring data used in decision-making about an individual is accurate). For these reasons, we find ABS arrangements (including reconciliation of statistical information where multiple forms are received from a single household) meet the requirements of APP 10. However, from a statistics standpoint, data accuracy may be improved in circumstances in which individuals feel free to be truthful. In our view, ensuring individuals are able to access a separate form if they wish may encourage respondent truthfulness and confidence in the process. No further issues identified.

5.5 Summary and recommendations

Generally, IIS finds that the option of a separate Census form offers a privacy sensitive approach to statistics collection. Stakeholders were also generally positive about the option and raised a number of questions about how use of a separate form would work in practice and whether individuals would have to inform others in the household about their use of a separate form.

During roundtable discussions, the ABS indicated that individuals would not have to inform other householders that they were filling out a separate form and that duplication across household and separate forms would be addressed during data processing with the separate form taking precedence in terms of the statistical information the ABS would collect into the Census dataset. We recommend the ABS develop consistent messaging on these and other matters outlined in Recommendation 5.

Recommendation 5 – Ensure communications materials and scripts address key questions about use of a separate Census form

Best practice

5.1 Develop consistent messaging on the following matters:

- How an individual can access a separate form.
- Whether an individual must inform others in their household that they are filling out a separate form.
- Whether it is allowable for an individual to fill out a separate form knowing their information will also be included in a household form.
- Whether an individual will 'get in trouble' if information about them supplied in the household form is inaccurate or inconsistent with information in the separate form.
- Which form takes precedence during ABS reconciliation processes (i.e. if an individual's information is included both in a household form and a separate form, which set of statistical information is recorded for the individual).

Best practice

5.2 Deploy consistent messaging about the option of separate Census forms in Census communications materials and Contact Centre scripts. Information about this option should be easy to find and not hidden or obscure. In determining the most appropriate forms of communication and outreach, take account of:

- Possible sensitivities and privacy risks of aligning the option of separate forms with the introduction to the Census of questions about gender and sexual orientation. (The ABS could consider consulting LGBTIQ+ groups on this issue.)
- Possible data processing and data quality challenges associated with possible high uptake of separate forms (including ensuring households fill out at least one household form rather than multiple personal forms).

6. Third party vendor management

The Phase 3 PIA is assessing the ABS's approach to third party vendor management (particularly in light of recent contractor breaches in connection with census activities in other countries). The purpose of this assessment is to ensure the ABS is doing everything it should be in relation to procurement and contract management to minimise the risk of privacy or security breaches perpetrated by third party service providers.

6.1 Background

The ABS has a range of internal governance arrangements in place to manage procurement processes. This includes the following general features:

- A Procurement Team that oversees engagement of vendors.
- A Contract Management Framework (currently under review).
- Support to the Contract Manager, as necessary, from the Procurement Team.
- A team-based process for checking contracts contain privacy and security related provisions.

In relation to Census procurement in particular, the ABS also has in place:

- A 2026 Census Program Procurement Strategy which outlines the ABS's approach to complex or high value procurements associated with the 2026 Census (including the Census Digital Service, mail house services, payroll for field staff, the Contact Centre, and data capture centres).
- A 2026 Census Procurement Oversight Group which was established to provide an additional level of review to support the Delegate(s) and the relevant Tender Evaluation Committee in complex procurement activity for the 2026 Census.
- A 2026 Census Register of Third-Party Agreements.
- A program of PTAs undertaken by the Census Privacy Team in collaboration with relevant business areas which assess third-party contracting arrangements.

6.2 Personal and other information involved

IIS reviewed the ABS's processes for managing vendors rather than focusing on a single vendor in particular. We understand that the ABS may use up to fifty third party service providers to support delivery of the Census. This can include providers of recruitment and workforce management software, providers of mail services, and providers of IT platforms to support collection and processing of Census forms.

The main types of personal information that vendors may handle during the Census (depending on their role) may be statistical information (i.e. personal information contained on Census forms); non-statistical information about individuals (e.g. information on the front of the Census form or information associated with Census-related enquiries); personal information about employees including members of the temporary workforce; and de-identified information. Details about the personal information a vendor may have to handle in the course of delivering services to, or on behalf of, the ABS, along with associated privacy and security obligations are specified during the procurement process and in contracts.

Contract Management Framework

The ABS has a Contract Management Framework in place supported by a range of tools, checklists and templates. The Framework establishes a risk-based approach to contract management creating three contract profiles: Light Touch (both low value and low risk exposure); Managed (either low value and low-medium risk or vice versa); and Fully Managed (both high risk and high value). Contract management requirements vary according to the contract profile. The Framework also incorporates 12 principles to guide Contract Managers and ensure governance and oversight is commensurate with the value and the risk associated with the contract.

Roles and responsibilities are set out in a number of the supporting documents, including the ABS Contract Management Framework Overview, the Contract Management Policy, the Contract Management Competencies and the Fully Managed Contract Plan. Generally, these document the roles of the Contract Owner and the Contract Manager, and at times also the Contract Management Group, Contract Administrators (ABS personnel) and the Procurement Manager.

6.3 APP analysis and other privacy risks

In assessing vendor management in light of Privacy Act requirements, IIS has given particular regard to APP 1 (implementing practices, policies and procedures that ensure agency compliance with the APPs). IIS has also considered APP 11 (Security of personal information stored or processed by third party vendors*)* and reasonable steps to safeguard personal information. In our view, the ABS is taking appropriate steps to meet APPs 1 and 11. The ABS has strong internal governance in place to ensure privacy and security is addressed in contracts and to oversee vendor activities.

As part of our assessment, IIS also reviewed a number of template contracts used by the ABS for particular vendor panels. All contracts contained standard privacy, confidentiality, security, and eligible data breach provisions. All contracts also contained a right to audit, including auditing of vendor compliance with privacy and security contract provisions. The Procurement Team informed IIS that these were baseline provisions and that during the contracting process, depending on the services being procured, additional project specific privacy and security requirements would be added to the contract as needed.

APP	*Comments and analysis*
APP 1	*Practices, procedures and systems to ensure APP compliance* APP 1 requires an agency to take reasonable steps to implement practices, procedures and systems that ensure APP compliance. In the case of procurement and contract management, an agency should have arrangements in place to ensure ongoing protection and appropriate handling of personal information when stored or processed by a third party provider. This includes ensuring inclusion of appropriate privacy and security provisions in contracts and ensuring strong contract management and oversight during the life of the contract. IIS reviewed the ABS's Contract Management Framework and associated policies, plans, templates and checklists (described in the sections above) and found these to be detailed, practical and thorough with clear articulation of roles and responsibilities for contract management. IIS also reviewed a number of contract templates used by the ABS (often in conjunction with procurement panels) and found that they all contained standard provisions pertaining to confidentiality, security, privacy, eligible data breach, and the right to audit. Most also specified particular security standards or requirements that the vendor must meet, such as ISO 27001, Infosec Registered Assessors Program (IRAP) assessment, the Protective Security Policy Framework (PSPF), and the Information Security Manual (ISM). The ABS advised that additional security requirements are added to contracts as needed, depending on the nature of the services to be delivered. Regarding Census procurement, the ABS also has a strategy in place with committee oversight. Below, we make some additional best practice suggestions the ABS could implement to strengthen vendor management – see Section 6.4. However, in terms of APP 1 compliance, IIS finds that the ABS is taking reasonable steps to meet APP requirements including when personal information is processed or stored by third party vendors. No further issues identified.
APP 11	*Security of personal information stored or processed by third party vendors* As noted in the row above, the ABS has standard provisions in its contracts that cover information security and usually bind the vendor to specific security standards or frameworks. Moreover, the ABS's Contract Management Framework takes a risk-based approach, providing for additional layers of oversight for 'Managed' and 'Fully Managed' contracts, including via the implementation of Fully Managed Contract Plans, intermittent Contract Health Checks and documenting and monitoring of risks via a dedicated Contract Risk Register. The ABS also advised that contractor security was considered in PTAs and in the team-based Census Data Protection and Retention Plans. It also advised that a Contract Manager can draw on the assistance of the Vendor Management Team in the Technology and Security Division for complex, high-risk contracts.

APP	Comments and analysis
	These arrangements appear comprehensive. However, IIS's assessment was largely 'on the papers' (noting that IIS was reviewing overarching arrangements rather than the security arrangements for a particular vendor) and it was difficult to determine how closely staff were following documented policies and checklists in practice and proactively monitoring vendor performance (from a privacy and security standpoint). To close any possible gap between intention and action, IIS recommends that ABS assessments or checks of vendor privacy and security compliance require confirmation in writing. See **Recommendation 6**.

6.4 Summary and recommendations

Overall, IIS finds that the ABS has a rigorous system in place for managing contracts. One possible area that the ABS could give attention to is proactive monitoring of vendor privacy and security compliance. This is already provided for in contract management policies and procedures. The purpose of Recommendation 6 is to build in added assurance that that monitoring is taking place in practice (in accordance with policies and procedures) at appropriate moments during the contract lifecycle and not only in response to an issue or incident. The degree of monitoring and oversight of vendor privacy will depend on the contract profile and nature.

In reviewing contract management arrangements, IIS observed that the Census Register of Third Party Agreements did not appear to be operating as intended. Currently, updating the register appears to be largely a clerical task which has little influence over the contracts themselves and their privacy-related provisions as those decisions have already been made by the time the register is filled out. IIS suggests that there may be opportunities to improve how the register operates in practice.

Recommendation 6 – Ensure strong assurance of vendor privacy and security compliance

Best practice

6.1 Ensure that, in updating the Contract Management Framework:

1. There is a mechanism requiring written confirmation by the Contract Manager of the proactive checks made of contractor (and subcontractor) privacy and security compliance for Managed and Fully Managed Contracts.
2. There is a mechanism requiring written confirmation by the Contract Manager or Contract Administrator that required security certifications, assessments or audit reports have been provided by the contractor and checked during onboarding or as appropriate.

The ABS has a number of vendor management arrangements in place. The purpose of this recommendation is to close any possible gap between intention and action by ensuring contract management policies and procedures (requiring monitoring and risk management) are being followed in practice. Strong assurance of vendor privacy and security compliance will be particularly important for 'Fully Managed' contracts involving handling of Census data or other personal information.

Best practice

6.2 Review the effectiveness of the 2026 Census Register of Third Party Agreements with a view to improving its operation and impact. In making improvements, the ABS could consider adjusting how it is used or filled out by Census teams; moving it to a different stage in the procurement process; or combining it with another governance mechanism to improve its operation.

7. Post enumeration survey

The Census Post Enumeration Survey (PES) is a household survey conducted shortly after each Census to provide an independent measure of Census coverage. The PES results are used to determine how many people should have been counted in the Census, how many people were missed (undercount) and how many were counted more than once or in error (overcount). The PES also measures the level of imputation error in Census processing.

The 2026 PES Main Event will approach approximately 55,000 households, while the Dress Rehearsal in 2025 will approach approximately 3,000. A very high response rate is required for the PES to estimate population and this rate needs to be consistent across all jurisdictions. To measure Census coverage, the PES team links PES data with Census data. During the lead up to the PES Main Event, the team prepares by testing linkage models and tools and conducting the Dress Rehearsal.

7.1 Changes expected in 2026

The PES will be carried out in a similar manner to previous iterations, however two changes for 2026 include:

- *PES Synthetic Test Dataset* – The ABS is developing a testing resource to support effective testing of the PES linking system. It is part of the Census 2026 Test Data Project which also includes development of a Census Synthetic Test Dataset to allow Census teams to test systems and processes using realistic (but synthetic) data.
- *Upgrades to PES systems and information infrastructure* – The PES team is preparing to change some of the tools, systems and platforms it uses for PES data processing. This includes likely use of ANDII for some parts of PES processing and use of new linkage tools, both for automated linking and clerical linking.

7.2 Personal and other information involved

Generally, the PES involves collection of:

- Name, age, sex, date of birth
- Country of birth
- Relationships between persons in the household
- Marital status
- Aboriginal and Torres Strait Islander status
- Whether the person usually resides in Australia or overseas
- Whether a person usually resides at the current dwelling or somewhere else
- Whereabouts on Census night and during the PES reference period (e.g. whether someone was away from current dwelling for some or all of the PES reference period).

PES synthetic dataset

The creation of a PES synthetic test dataset involves use of the above data variables from the 2021 PES and 2021 Census but with synthetic name and address data so that the information is rendered de-identified. The ABS advised that the method used to synthesise addresses is irreversible. That is, there is no retained concordance between the original and the synthetic address. The addresses are real addresses extracted from the Address Register, which are randomly assigned to unit records. The ABS further advised that measures are in place to ensure that none of the synthesised address data is, by chance, the same as the original address or similar enough to the original address to allow reidentification to occur.

The ABS conducted a PTA on the PES synthetic dataset project which reviewed the project from a privacy standpoint and outlined the security protections that will apply to the dataset. IIS found the PTA to be detailed and rigorous and made clear that strong security and access arrangements would apply to the PES synthetic dataset at all stages of its use and storage. We also note that the dataset does not meet the definition of personal information and is therefore not subject to the APPs. No further issues were identified.

Upgrades to PES systems

The PES involves conducting a follow up survey after the Census main event to check the accuracy of Census data and population estimates. It is primarily conducted via a computer aided telephone interview with a small proportion conducted via computer enabled personal interview. There are no webforms or paper forms for the PES. IIS understands that none of these activities will be changing in 2026.

The PES data must then be linked to Census data to check Census enumeration accuracy. This linkage activity is also the same as in previous years and supports the primary purpose that the PES data was collected. What is changing are the linking tools (and supporting platforms and environments) that the ABS will use for PES linkage. Work on PES systems is ongoing but, at the time of writing, changes include changes to:

- *Linking tools* – use of new linking tools to facilitate automated linking.
- *Supporting platforms for automated linking* – some changes to platforms and environments in which automated linking will take place.
- *Supporting platforms for manual linking* – some changes to platforms and environments in which manual linking will take place.
- *File transfer* – some changes to file transfer arrangements and monitoring to strengthen security as data moves between environments.

IIS understands that PES data processing involves the following main activities:

- *Pre-processing* – PES and Census datasets are pre-processed to put the datasets into a form that allows for linking.
- *Automated linking* – PES and Census datasets are linked using an automated linkage tool.

- *Post-linkage processing* – the linked files are processed again to determine the quality of the links (whether platinum, silver or tin); platinum links are accepted, tin are discarded and silver are submitted to human review.
- *Manual review and linking* – temporary coding staff review and confirm or discard 'silver'.
- *Weighting and estimation* – following linkage activity, Census data is updated with finalised counts (including imputed persons); PES data is then aligned to Census counts and fed into an estimation system to calculate estimates of population and Census undercount.

7.3 APP analysis and other privacy risks

In conducting the APP analysis for the PES, IIS has focused on those parts of the PES that will be different in 2026. As noted above, this includes changes to systems, tools and platforms which affect how PES information is used and stored. For APP purposes, this means that the relevant APPs that apply in this case are APPs 6 (Use) and 11 (Security). The data processing also involves activities that go to data accuracy and quality, so APP 10 (Data quality) has been considered as well.

APP	*Comments and analysis*
APP 6	*Use of PES data* APP 6 states that an agency must only use personal information for the primary purpose it was collected unless an exception applies. IIS understands that the primary purpose of conducting the PES is to provide an independent measure of Census coverage (to determine the degree of undercount) and level of imputation error. To achieve that purpose, PES data must be linked with corresponding Census data. As outlined above, this involves five main data processing activities: pre-processing, automated linking, post-linkage processing, manual linking, and weighting and estimation. While some of the tools and platforms used for these activities have changed since the 2021 Census, the data processing activities remain very similar to years past and serve the same ends. IIS finds that these activities fall within the primary purpose of collection and therefore meet APP 6. No further issues identified.
APP 6	*Use of Census data for PES-related purposes* It was not clear to IIS whether use of Census data for PES-related purposes fell within the 'primary purpose' of the collection of Census data or whether it constituted a 'secondary use' of the data. If this use of Census data does constitute a secondary use, IIS believes it meets the exception contained within APP 6.2(a) which allows use of personal information for a secondary purpose if that purpose is related to the primary purpose of collection and is likely to be within the individual's reasonable expectations. IIS believes that it is likely that individuals would expect the ABS to have processes in place to check or verify the accuracy of Census data and population counts. IIS also notes that the ABS's usual

APP	Comments and analysis
	practice is to include information about the PES both in the Census Privacy Statement and on a dedicated webpage – this also goes to establishing 'reasonable expectations.' No further issues identified.
APP 10	*Quality of personal information* APP 10 states that an agency must take reasonable steps to ensure that the personal information it collects and uses is accurate. The intended use of Census information for statistical purposes is relevant to the interpretation of this principle. Given that there is no direct impact on the individual regarding inaccurate Census information, the privacy impact is significantly reduced. So, the steps that are 'reasonable' for the purposes of APP 10 might be lesser than in a case where inaccurate information may have a direct, adverse impact on an individual. IIS finds, therefore, that steps to ensure data accuracy will be driven by statistical objectives (i.e. ensuring data used in the production of statistics is accurate) rather than privacy ones (i.e. ensuring data used in decision-making about an individual is accurate). It is worth noting that the PES's main purpose is to enhance the quality and accuracy of Census data. IIS also notes that the ABS has arrangements in place to allow for human review of possible low-accuracy linkages between the PES and Census datasets. In light of these factors, IIS finds that PES arrangements meet the requirements of APP 10. No further issues identified.
APP 11	*Security of PES-related information* APP 11.1 requires an agency to take reasonable steps to protect the personal information it holds against misuse, interference and loss, and from unauthorised access, modification and disclosure. IIS has reviewed the changes to tools and processing environments that will be used to conduct the PES. In our view, the changes overall appear to strengthen rather than diminish data security. The use of the ANDII moves linking activity to an environment that has undergone rigorous security testing and PIA review. The ABS has also taken, or is taking, steps to ensure file transmission between environments is secure and appropriately monitored. IIS understands that PES roles and access restrictions have been documented and will be implemented accordingly. IIS further understands that early security assessments have been undertaken and that security will continue to be tested and reviewed in the lead up to the Census and PES main events. Security arrangements are also being reviewed and documented via a PTA process which is, at the time of writing, ongoing. It is outside the scope of this PIA to conduct a security assessment of PES systems. However, in reviewing ABS arrangements, IIS finds that the ABS appears to be taking a

APP	Comments and analysis
	robust approach to information security and has strong internal security governance in place to ensure proactive identification and control of risk. No further issues identified.
APP 11	*Retention of PES-related information* The ABS advised that retention of PES-related information will follow the same timelines for name and address deletion as for Census data. The ABS also advised that these disposal dates will be recorded in PES section Data Retention Plans for PES data and for Census data. No further issues identified.

7.4 Summary

IIS assessed PES data processing arrangements for 2026 with a particular focus on those arrangements that will be new or different compared to the previous Census. From our review, activities and objectives remain largely the same, while some of the tools and platforms are different (resulting in some different internal dataflows). From a compliance standpoint, we find the ABS is meeting its obligations under the APPs though acknowledge that, at the time of writing, PES arrangements were still being finalised, with a PTA underway.

8. Census refusals process

Within the Customer Service team, the Refusals team manages cases where an individual refuses to complete a Census form. Under the Census and Statistics Act, individuals must complete (or have their information included in) a Census form – in other words, completing a Census form is mandatory not voluntary. Cases of refusal are assessed by the ABS and either closed or pursued, depending on the circumstances of the refusal.

8.1 Changes expected in 2026

The refusals system at the ABS will continue in largely the same form as the past Census but with two possible changes:

- *Adoption of a new platform for processing refusals* – the ABS plans to use a cloud-based platform (the new platform) to process Census refusals. The move to the new platform is motivated by a need to improve the reliability and functionality of the refusal case management system.
- *Development of a policy for classifying paper-form based refusal* – the ABS is at an early stage of considering whether to develop an internal policy on establishing thresholds for Census refusal involving incorrectly filled out, or vandalised, paper forms.

8.2 Personal and other information involved

The refusals process does not involve statistical information. Generally, it involves the following personal information:

- Name, address and date of birth
- A record of ABS engagement with an individual (for example, details of correspondence between the ABS and the individual).

Use of the new platform for refusals case management

IIS understands that the ABS already uses the new platform for other internal functions and that its use for refusals would constitute an additional separate use of the platform with its own workflows and access permissions. The ABS explained that during the 2021 Census, the system used for refusals struggled to cope with demand and hindered the processing of refusals, hence the decision to upgrade to the new platform.

The refusals process will broadly be the same as previously. Individuals can communicate their intention to refuse to complete a Census form either by calling the Census Call Centre or by telling a field officer. Census Call Centre staff input details of the refusal into their case management system which transfers the information to the new platform. Or, field officers submit details of the refusal via the field officer app, which transmits the information to the new platform. Refusal information is also transmitted to the Census enumeration management system.

The new platform creates a refusals case and assigns staff to process predefined stages of the refusal workflow. This may include checking the refusal is a refusal and has not been entered in error; following up with the individual to encourage Census form completion; considering extenuating circumstances or reasons for non-compliance; sending a notice of direction to the individual; and, if other options to encourage compliance fail, pursuing prosecution.

IIS understands that these activities are largely the same as years past but will now take place using the new platform. IIS also understands that a PTA is currently underway.

Development of a policy for classifying paper-form based refusal

The ABS is at an early stage of considering whether to formalise a policy for classifying paper-form based refusal. These are cases where an individual returns a paper form in a form that is equivalent to a refusal – providing responses that are obviously false or otherwise vandalising the form. Currently the Refusals team deals with these forms ad hoc and generally only vandalised forms are flagged as possible refusals for follow-up. A more systematic approach to identifying these forms would allow the Refusals team more time to follow-up with individuals who have filled in a paper form this way and seek compliance before Census deadlines.

IIS understands that the team responsible is still at an early stage of considering how such a policy might work in practice and that no final decision has been made whether to go ahead. We have offered some analysis below on possible APP considerations, noting project uncertainty.

8.3 APP analysis and other privacy risks

In conducting the APP analysis, IIS focused on those matters that are changing in 2026. The upgrade to internal case management systems mostly goes to the application of APPs 6 (Use), and 11 (Security). Development and implementation of a policy on paper-form based refusal mostly goes to the application of APPs 5 (Notice), 6 (Use), and 10 (Data quality). IIS understands that collection of personal information in connection to processing refusals is not changing.

APP	Comments and analysis
APP 5	*Transparency about consequences of filling out a Census form with incorrect information* The ABS is considering formalising a policy on classifying refusals involving intentionally including incorrect information in a paper Census form. In effect, this may mean that forms that have previously been accepted by the ABS might be classified as refusals and followed up accordingly. IIS assessed whether this would affect notice requirements under APP 5. In particular, APP 5.2(e) requires an agency to make an individual aware of the main consequences (if any) for the individual if all or some of the personal information is not collected by the agency. IIS reviewed the previous (2021) Census Privacy Statement and finds that the ABS already includes information explaining not only that failure to participate in the Census may result in penalties, including fines, but also that provision of incorrect or misleading information may also result in penalties. This would appear to cover the ABS's activities in this area, including introduction of a more systematic approach to identifying form-based refusals. As long as the ABS follows the same notice approach again, it will be acting in accordance with APP 5. No further issues identified.
APP 6	*Processing of refusals using the new platform* A central change for Census 2026 is that the ABS will use the new platform to process refusals. Refusals enter the new platform either via the call centre or via field officers. The new platform creates a case and workflow for each refusal which allows for ABS review of the refusal, follow-up with the individual, sending of a notice of direction to the individual, and, in limited cases, disclosure of relevant information to the Commonwealth Director of Public Prosecutions for possible prosecution. APP 6 requires an agency to only use personal information for the primary purpose it was collected unless an exception applies. IIS reviewed the internal processing of refusals (outlined above) and finds that internal use aligns with the primary purpose of collection which is to process Census forms (in order to conduct the Census) and pursue enforcement under the Census and Statistics Act as necessary. Internal use of personal information, while facilitated by a new platform, appear to be the same as in previous Censuses. From IIS's review, there did not appear to be any new secondary uses or disclosures planned. No further issues identified.
APP 6	*Use of Census forms for refusal processing* As outlined above, the ABS is considering formalising a policy on classifying refusals involving intentionally including incorrect information in a paper Census form. In effect, this may mean that forms that have previously been accepted by the ABS might be classified

APP	Comments and analysis
	as refusals and followed up accordingly. IIS assessed whether this might constitute a new 'use' of personal information included in Census forms and whether that use aligned with the requirements of APP 6. We find, first, that the ABS has already used personal information included on Census forms in this way – previously it has processed vandalised forms as refusals. The main difference in adopting an internal policy for identifying form-based refusals would be moving from an ad hoc approach to a more systematic approach. Second, we find that this use of personal information contained in Census forms to identify and process refusals meets the requirements of APP 6 – specifically APP 6.2(a) which permits use of personal information for a secondary purpose related to the primary purpose of collection which is likely to be within the individual's reasonable expectations. The Census is compulsory under the Census and Statistics Act and one aspect of running the Census is enforcing individuals' obligations under the Act. We therefore find that this constitutes a related secondary use of personal information collected for the Census. The compulsory nature of the Census which has been running for decades is widely known in the community and is advertised in the lead up to each Census. In addition, information about the compulsory nature of the Census and penalties for refusing to participate is given in the Census Privacy Statement. These factors go to establishing reasonable expectations. No further issues identified
APP 10	*Ensuring accuracy of refusals-related personal information* APP 10 states that an agency must take reasonable steps to ensure that the personal information that the agency uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant. APP 10 may have relevance for any policy the ABS develops on identifying form-based refusals. For example, given the possible adverse impact on the individual of a finding that a returned form is a refusal, it would be reasonable for the ABS to identify form-based refusals with a high degree of accuracy. IIS suggests that the ABS take this into account if it proceeds with developing and implementing a policy for identifying form-based refusals – that is, the ABS should only classify forms as refusals where it has a high degree of certainty that the form contains intentionally incorrect information. No further issues identified.
APP 11	*Security of personal information stored and processed in the new platform* APP 11.1 requires an agency to take reasonable steps to protect the personal information it holds against misuse, interference and loss, and from unauthorised access, modification and disclosure. IIS understands that the ABS's use of the new platform will occur in accordance with the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM). All data is stored onshore. IIS further understands that the PSPF

APP	Comments and analysis
	and ISM also govern the use and configuration of auxiliary systems. The ABS advised IIS that the System Security Plan sets out user roles and access privileges for the new platform, and that role-based access will apply, including access restriction and monitoring. The ABS also advised that personnel with administrative and privileged access to the new platform will sign a Deed of Confidentiality prior to gaining access to ABS ICT systems. Such staff will undergo personnel security vetting and clearance checks in accordance with the ABS's protective security requirements and the classification of the data, with Australian citizenship and Baseline Security clearance as minimum requirements. It is outside the scope of this PIA to conduct a security assessment of the ABS's use of the new platform for refusals processing. However, in reviewing ABS internal information security governance, IIS finds that such arrangements appear to be operating effectively with active consideration and implementation of controls to mitigate risks and ensure strong access management. IIS also notes that the ABS is currently conducting a PTA which also identifies and addresses privacy and security risks and controls. No further issues identified.
APP 11	*Retention of refusals-related personal information in the new platform* APP 11.2 requires an agency to dispose of personal information it no longer needs (for a purpose permitted under the APPs), other than personal information contained in a Commonwealth record. Most of the ABS's records are Commonwealth records and are governed by a range of Record Authorities issued by the National Archives of Australia including but not limited to ABS Records Authority and Administrative Functions Disposal Authority (AFDA) Express v2. IIS understands that refusals information stored in the new platform will be disposed of in accordance with the relevant Records Authority with retention periods varying depending on the category of information. The ABS advised that the data disposal process will likely involve the Census Customer Service team raising a request for technical staff to delete the data and provide evidence of the deletion (such as a deletion log). However, the new platform for refusals is still being set up and deletion protocols will be confirmed as the project proceeds via the PTA (currently in progress). IIS also understands that data retention periods and requirements for refusal-related information are documented in the Census Customer Service team's Census Data Protection and Retention Plan. No further issues identified.

8.4 Summary

IIS reviewed the new refusals system arrangements against the requirements of relevant APPs and finds the ABS's approach aligns with APP requirements – noting that, at the time of writing, the ABS is still in the process of building the refusals system on the new platform and that an internal PTA is ongoing. IIS observes that any changes to how the ABS identifies or classifies form-based refusals should ensure a high degree of confidence when assigning a Census form as a refusal – this will ensure compliance with APP 10.

9. Privacy Act reforms

The Privacy Act has recently been amended with an initial tranche of reforms arising from the 2022 Review of the Privacy Act overseen by the Attorney-General's Department. In light of this, the ABS asked IIS to consider whether there were any amendments to the Privacy Act that it should take into account with regard to Census operations.

9.1 Summary of key reforms

Some of the key reforms made to the Privacy Act include the following:

- *Codes, powers and enforcement* – Amendments to the Privacy Act now enable the Minister to direct the Information Commissioner to develop and register an APP code. There have also been reforms to penalty provisions to enable the Commissioner to take enforcement action against a serious (but not repeated) interference with privacy and to expand the Commissioner's enforcement options with regard to other interferences with privacy and breaches of prescribed APPs.
- *Children's Online Privacy Code* – New provisions introduced to the Privacy Act require the Information Commissioner to develop and register an APP code about online privacy for children within 24 months. The code will apply to providers of social media services, relevant electronic services or designated internet services which are likely to be accessed by children.
- *Emergency and eligible data breach declarations* – The Privacy Act allows the Minister to make an emergency declaration which allows greater sharing of personal information during emergencies or disasters. Amendments to those provisions introduce greater specificity to declarations. New eligible data breach declarations also allow the Minister to make a declaration which, similar to an emergency declaration, permits sharing of personal information to prevent or reduce the risk of harm to individuals.
- *Overseas data flows* – Amendments to APP 8 allow the Minister to prescribe countries and binding schemes which protect personal information in a way that, 'overall, is at least substantially similar to the way in which' the APPs protect information. APP 8.2 then permits disclosure to those overseas jurisdictions.
- *Automated decision-making and privacy policies* – Amendments to APP 1 require an agency to include information about its automated decision-making activities in its privacy policy. (See Section 9.2 below.)
- *Statutory tort for serious invasions of privacy* – The introduction of a privacy tort allows individuals to sue for a serious invasion of privacy where the invasion was reckless, serious in nature, and outweighed any public interest in the invasion. (See Section 9.3 below.)

In addition, the Criminal Code has been updated to include:

- *Doxxing offences* – New doxxing provisions introduce a criminal offence for malicious release of personal information.

On reviewing those Privacy Act changes outlined above, IIS found that most had no or little material impact on the ABS and its operations.

9.2 Automated decision making and privacy policies

Amendments to the Privacy Act include an additional privacy policy requirement under APP 1, however that requirement does not come into effect until December 2026.

New provisions

The amendment will require an agency to include information about any automated decision-making it undertakes in the agency's APP privacy policy. Automated decision-making is narrowly defined to cover cases where:

- the entity has arranged for a computer program to make, or do a thing that is substantially and directly related to making, a decision;
- the decision could reasonably be expected to significantly affect the rights or interests of an individual; and
- personal information about the individual is used in the operation of the computer program to make the decision or do the thing that is substantially and directly related to making the decision.

If the automated activity meets those requirements, the agency must include the following information in its privacy policy:

- the kinds of personal information used in the operation of such computer programs
- the kinds of decisions made solely by the operation of such computer programs
- the kinds of decisions for which a thing, that is substantially and directly related to making the decision, is done by the operation of such computer programs.

Impact on the administration of the Census

These provisions will not affect the ABS's arrangements for the 2026 Census as they do not come into effect until December 2026. Despite this, IIS reviewed the ABS's Census activities and arrangements to offer advice on future automated data processing activities but did not identify any activities that meet the new Privacy Act definition of automated decision-making. For example, the Phase 2 Census PIA covered the WoAG Coding Capability however the coder does not impact the rights or interests of the individual, and the data processing is conducted using de-identified information. Therefore, the new privacy policy obligations regarding automated decision-making will not apply in that case.

If the ABS were to use automated decision-making to process form-based refusals (that is, cases where an individual has vandalised a Census form or otherwise intentionally submitting incorrect information), then this activity may trigger the application of the new privacy policy requirement. For the avoidance of doubt, the ABS has not indicated any intention of using automated decision-making in this way – this simply provides an example of when these provisions may apply.

To prepare for December 2026 (when these provisions take effect) we suggest the ABS update its internal PTA template to include a question about whether the new activity or proposal under consideration will involve automated decision-making. Depending on the circumstances, if automated decision-making is involved, some further privacy analysis may be required to check privacy compliance. The aim would be to ensure new developments in this area are identified (and covered in the ABS's privacy policy) and any risks are addressed.

9.3 Tort for serious invasions of privacy

The recent reforms to the Privacy Act introduced a new tort for serious invasions of privacy.

New provisions

The new provisions state that an individual (the plaintiff) has a cause of action in tort against another person (the defendant) if:

- the defendant invaded the plaintiff's privacy by doing one or both of the following:
  - intruding upon the plaintiff's seclusion
  - misusing information that relates to the plaintiff and
- a person in the position of the plaintiff would have had 'a reasonable expectation of privacy in all of the circumstances and
- the invasion of privacy was intentional or reckless and
- the invasion of privacy was serious and
- the public interest in the plaintiff's privacy outweighed any countervailing public interest.

The Privacy Act defines 'countervailing public interest' to include:

- freedom of expression, including political communication and artistic expression
- freedom of the media
- the proper administration of government
- open justice
- public health and safety
- national security
- the prevention and detection of crime and fraud.

In addition, the Privacy Act includes a range of other defences including where the invasion of privacy was required or authorised by law or where it was necessary to prevent or lessen a serious threat to the life, health or safety of a person.

Impact on the administration of the Census

IIS believes this provision will have a negligible impact on agencies, like the ABS, which already comply with the APPs and have mature privacy and security governance arrangements in place. The new privacy tort addresses *serious* invasions of privacy and as such creates a high bar for action under its terms. For example, for an action to be brought, the invasion of privacy must have been intentional and reckless – this means that a data breach occurring despite an agency's best efforts to protect the personal information it holds would not meet the 'intentional and reckless' requirement. Any agency that complies with APP 11 is in a strong position to defend itself on this count. Moreover, the new provisions include the defence that the invasion of privacy was required or authorised by law. This means the permissions granted by the Census and Statistics Act should also act protect the ABS from action under the new privacy tort provisions.

Generally, IIS finds that the ABS is taking appropriate steps to comply with its Privacy Act obligations and manage privacy risk. No further issues or actions related to this matter were identified.

9.4 Other reforms

New enforcement powers and penalty provisions

The new enforcement powers and penalty provisions have been implemented to give the Information Commissioner more flexibility to address interferences with privacy that do not meet the 'seriousness' threshold that would otherwise have restricted imposition of penalties. The new penalty provisions underscore the importance of privacy compliance. IIS found that through this PIA process and the ABS's internal privacy processes, the ABS is taking appropriate steps to ensure it operates within the bounds of the Privacy Act and the APPs.

New doxxing provisions

Doxxing refers to the malicious publication of an individual's personal details – usually to allow intimidation or harassment of the individual. IIS believes the ABS has appropriate controls in place to protect the personal information it holds from intentional misuse. This includes role-based access controls for systems that store personal information and system monitoring to detect unusual or unauthorised activity, along with storage of data in de-identified form or with functional separation of data from identifiers. The ABS also imposes security clearance requirements on most roles with access to Census data and trains staff on privacy obligations.

Appendix A. Glossary

Abbreviation or term	Expansion or definition
ABS	Australian Bureau of Statistics
ABS Act	*Australian Bureau of Statistics Act 1975 (Cth)*
ACLD	Australian Census Longitudinal Dataset
Administrative data	Administrative data is information collected by government agencies, businesses or other organisations for various purposes, including registrations, transactions and record keeping, usually during the delivery of a service.
AI	Artificial Intelligence
ANDII	Australian National Data Integration Infrastructure
APPs	Australian Privacy Principles
APS	Australian Public Service
BETA	Behavioural Economics Team of the Australian Government
BLA	Business Locations Asset
CAT	Census Agent Tool
CIPA	Census Independent Privacy Advisor
CoATSIS	Centre of Aboriginal and Torres Strait Islander Statistics
DAT Act	*Data Availability and Transparency Act 2022 (Cth)*
DATA Scheme	The data sharing scheme established by the DAT Act
EMI	Enumeration Management System
IIS	IIS Partners (report author)
IRAP	Infosec Registered Assessors Program
ISM	Information Security Manual
NDDA	National Disability Data Asset
OAIC	Office of the Australian Information Commissioner
ORE	Operational Readiness Exercise
PES	Post Enumeration Survey
PIA	Privacy Impact Assessment

Abbreviation or term	Expansion or definition
PLIDA	Person Level Integrated Data Asset
Privacy Act	*Privacy Act 1988 (Cth)*
PSPF	Protective Security Policy Framework
PTA	Privacy Threshold Assessment
SADE	Scaled Analytical Data Environment
SEAD	Secure Environment for Analysing Data
WoAG	Whole of Australian Government

Appendix B. Documents reviewed and meetings held

B.1 Documents reviewed

Documents reviewed
1. Various internal privacy threshold assessments related to Census operations
2. Privacy Impact Assessment - 2026 Census Temporary Workforce Recruitment System - v.3 approved by Census GM.pdf
3. 2026 Census Data Protection Plan_February2025.docx
4. 2026 Census Register of Third Party Agreements.JPG
5. 2026 Census XXXXX Section Data Protection and Retention Plan and Privacy Action Plan TEMPLATE v2.1.docx
6. PIA Phase 3 - PI Questionnaire - Inclusive Strategies and Engagement.docx
7. PIA Phase 3 - PI Questionnaire - Census Communication.docx
8. PIA Phase 3 - PI Questionnaire - Census Communication_17062025updated.docx
9. PIA Phase 3 - PI Questionnaire - Census Coverage and Data Quality .docx
10. PIA Phase 3 - PI Questionnaire - Data Capture Centre.docx
11. PIA Phase 3 - PI Questionnaire - Workforce Services.docx
12. PIA Phase 3 - PI Questionnaire Address Register.docx
13. PIA Phase 3 - PI Questionnaire Business Location Asset.docx
14. PIA Phase 3 - PI Questionnaire CADV- V2.0.docx
15. PIA Phase 3 - PI Questionnaire CADV.docx
16. PIA Phase 3 - PI Questionnaire Census Enumeration.docx
17. PIA Phase 3 - PI Questionnaire Content Development.docx
18. PIA Phase 3 - PI Questionnaire Customer Service.docx
19. PIA Phase 3 - PI Questionnaire Data Design.docx
20. PIA Phase 3 - PI Questionnaire Data Release, User Support and Research.pdf

Documents reviewed
21. PIA Phase 3 - PI Questionnaire Digital service.docx
22. PIA Phase 3 - PI Questionnaire -Logistics Mail Print Capture.docx
23. PIA Phase 3 - PI Questionnaire Post Enumeration.docx
24. PIA Phase 3 - PI Questionnaire Statistical Geography.docx
25. 5146-B - Privacy consultation Plain Language 270623.pptx
26. A. NDDA ANDII Privacy Consultation Report_Final_21.11.23.pdf
27. ABS Risk and Benefit Framework - Template - v1.0.pdf
28. ABS Risk and Benefit Framework v1.0.pdf|
29. Attachment A - Census Decision Process - Final.docx
30. B. NDDA and ANDII PIA Report_Final_29.11.23.pdf|
31. DRC 11 June 2024 - Paper - Final v3.docx
32. FINAL SENTTopic Response 2026 Census PIA_DATA Scheme and NDDA v2.docx
33. NDDA De-Identification Strategy v.1.00 - Endorsed.pdf
34. NDDA planned Datasets.pptx
35. Overview of PLIDA and NDDA comparison_extract from researcher guide.pptx
36. CWS - Newstarter Systems and Privacy expectations.PNG
37. Recruitment Training Module - Privacy Content.docx
38. Remote_Paper Pathway_Hiring Manager Privacy.pdf
39. 20250131 ABS Census Test Report Round 2.1 Final.pdf
40. 20250204_Census use of administrative data - Comms plan_AK_Draft.pdf
41. 2025Jan ABS Census Test Report Round 1 v3 final (003).pdf|
42. 2026 Census - BETA Project Scope 01042025.pptx|
43. Engagement agreement ABS Census user testing v3_14012025.docx
44. Business Rules for use case 1.docx

Documents reviewed
45. Draft article on admin data use.docx
46. Income variables- draft.docx
47. MotorVehiclePTADiagrams_v4_7Feb2025.pptx
48. 2023 CDC Head Agreement.pdf
49. 2026 Census Procurement Oversight Group_ToRv1.5_March 2025.docx
50. 2026 Census Program Procurement Strategy v5March 2023.docx
51. 21.12.2020 FINAL- Cloud Marketplace Head Agreement (Preferred Tenderer Version) (3).pdf
52. ABS - Contract Implementation Checklist 010425.docx
53. ABS - Contract Management Summary v04Mar25.docx
54. ABS - Fully Managed Contract Management Plan 010425.docx
55. ABS Contract Management Competencies .docx
56. ABS Contract Management Overview.docx
57. ABS Contract Management Principles .docx
58. ABS Long-form Services Contract Template May 23 .docx
59. Cloud marketplace contract template.pdf
60. KB0018272 Contract Management.docx
61. Knowledge Document Page.docx
62. MAS Head Agreement - July 2023 (3).pdf
63. PP Phase 2 Head Agreement.pdf
64. LGBTIQ+ EAC_Dec 2023_Summary of Subgroup activity - FINAL.docx
65. LGBTIQ+ EAC_NOV 2024 _Summary of Subgroup activity FINAL.pdf
66. Notification ABS Expert Advisory Committee Round Two Testing Outcomes SECOFFICIALSensitive.msg
67. Round Table May 2024 Session 10 - 2026 Census Content .docx
68. Basic and detailed microdata release - instructions.pdf

Documents reviewed
69. Safe Data Risk Assessment for data shared with ABS via DAT Act 2022 Scheme.pdf
70. Simplification of direct endorsement criteria [SEC=0.pdf
Information Flow Diagrams
71. PIA Phase 3 - CADV.pptx
72. PIA Phase 3 - CDS.pdf
73. PIA Phase 3 - Census Content v.3.vsdx
74. PIA Phase 3 - Census Coverage and Data Quality V1.0.pdf
75. PIA Phase 3 - Census Coverage and Data Quality V2.0 .pdf
76. PIA Phase 3 - Census Coverage and Data Quality V3.0.pdf
77. PIA Phase 3 - Census Dissemination .pdf
78. PIA Phase 3 - Census Workforce Services- Detailed.pdf
79. PIA Phase 3 - Census Workforce Services.pdf
80. PIA Phase 3 - Command Centre Strategic.pdf
81. PIA Phase 3 - Contact Centre and Customer Support process mapping.pdf
82. PIA Phase 3 - Data Capture - Warehouse Flow.pdf
83. PIA Phase 3 - Data Design.pdf|
84. PIA Phase 3 - Data maps Census and Statistical geography .png
85. PIA Phase 3 - Overall Warehouse Flow.pdf
86. PIA Phase 3 - Post Enumeration Survey (PES) V4.pdf|
87. PIA Phase 3 - Refusals process mapping.pdf
88. PIA Phase 3 -Refusals and corro.pdf
89. PIA Phase 3 - Contact Centre and Customer Support process mapping.pdf

B.2 Meetings held with ABS and stakeholders

Meetings held	Date
Sharing 2026 Census data under the Data Availability and Transparency Act 2022 (DAT Act)	1-May-25
Census Workforce Services	1-May-25
Communications Team	2-May-25
Census Dissemination	2-May-25
Administrative data use for 2026 Census focusing on use of administrative data (use case 3)	2-May-25
Refusals process	5-May-25
Coding Redevelopment	5-May-25
Access to a personal form	5-May-25
Post Enumeration Survey (PES)	6-May-25
Census Digital service and myGov	6-May-25
Third party vendors – Management and Privacy risks	8-May-25
Census Content Development	8-May-25
Location Data Engineering	9-May-25
Roundtable - 1	11-Jun-25
Roundtable - 2	13-Jun-25
Follow-up with administrative data	17-Jun-25
Meeting with OAIC	10-Jul-25

Appendix C. External stakeholders consulted

Two roundtables were held to discuss privacy considerations associated with the Census with eleven external stakeholders participating in the discussion. This included representatives from the following organisations:

- Data Standards
- Department of Education
- Department of Employment and Workplace Relations
- Faculty of Law and Justice, University of New South Wales
- Griffith Data Trust and Relational Insights Lab
- Griffith University
- LGBTIQ Health Australia
- Queensland Union of Civil Liberties
- SBA Lawyers and Vecor Technologies
- Standards Australia

The ABS and IIS also met with, or received a submission from, the Office of the Australian Information Commissioner and the Office of the Victorian Information Commissioner.

INFORMATION INTEGRITY SOLUTIONS PTY LTD
PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438
E: contact@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN 107 611 898

IIS Partners
INFORMATION INTEGRITY SOLUTIONS